وزارة التعليم العالي والبحث العلمي
جامعة أكلي محند أولحاج
-البويرة-
كلية الحقوق والعلوم السياسية

Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique
Université Akli Mohand Oulhadj - Bouira -
Tasdawit Akli Muḥend Ulḥağ - Tubirett -
Faculté de droit et des sciences politiques

النظام القانوني للإثبات الإلكتروني

أطروحة لنيل شهادة دكتوراه " علوم " في الحقوق

تخصص قانون خاص

إعداد الطالبة **إشراف الأستاذ الدكتور**

بن علي نريمان **ناصر حمودي**

أعضاء لجنة المناقشة

اللقب والاسم	المؤسسة الأصلية	الصفة
أ.د/ مخلوف كمال	جامعة أكلي محند أولحاج–البويرة	رئيسا
أ.د/حمودي ناصر	جامعة أكلي محند أولحاج–البويرة	مقررا
أ.د/ طيبي أمقران	جامعة أكلي محند أولحاج–البويرة	ممتحنا
د/ موكة عبد الكريم	جامعة محمد الصديق بن يحيى– جيجل–	ممتحنا
د/براهيمي جمال	جامعة مولود معمري– تيزي وزو–	ممتحنا
د/ خليفي سمير	جامعة أكلي محند أولحاج–البويرة	ممتحنا

السنة الجامعية 2022/2021

- قال عبد الرحيم البيساني -

" إني رأيت أنه لا يكتب إنسان كتابا في يومه، إلا قال في غده: لو غُيِر هذا لكان أحسن، ولو زيد هذا لكان يستحسن، ولو قدم هذا لكان أفضل، ولو ترك هذا لكان أجمل، وهذا من أعظم العبر وهو دليل على استيلاء النقص على جملة البشر".

إهداء

إلى روح والدي الطاهرة الزكية،

إلى نبع الحنان والدتي أطال الله في عمرها،

إلى زوجي الكريم، سندي ومتكئي في هذه الحياة والذي قاسمني التعب من

أجل إخراج هذا العمل في صورته النهائية،

إلى فلذتي كبدي، إيلين وإسحاق، اللذين قصرت في حقهما من اللعب

والمرح من أجل إتمام هذا العمل،

إلى من أشد بهم أزري أخواتي،

إلى كل عائلتي،

إلى كل أساتذتي وأصدقائي وأحبائي،

إلى كل من أعانني على إنجاز هذا العمل من قريب أو من بعيد،

أهدي ثمرة عملي المتواضع .

نريمان

شكر وعرفان

الحمد لله الذي علم الإنسان ما لم يعلم، أشكره و أثني عليه إذ أعانني ويسر لي السبيل

حتى فرغت بفضله و حمده و توفيقه من إعداد هذه الأطروحة

و بمقتضى واجب الاعتراف بالفضل، أذكر بكل الخير والعرفان، وأتقدم بالشكر و الامتنان ، مع فائق احترامي و تقديري للبروفيسور - ناصر حمودي- لتفضله بالإشراف على هذه المذكرة ، وحرصه ومتابعته المستمرين، وملاحظاته وتوجيهاته القيمة.

كما أتقدم بالشكر لأعضاء لجنة المناقشة، لقبولهم مناقشة هذا العمل

نريمان.

﴿قائمة أهم المختصرات﴾

أولاً- باللغة العربية

ق. م. ج:.....قانون مدني جزائري

ق. ت. ج:.....قانون تجاري جزائري

ق. ع. ج:.....قانون عقوبات جزائري

ق. إ. م. إ:.....قانون الإجراءات المدنية والإدارية

د. د. ن:.....دون دار نشر

د. س. ن:.....دون سنة نشر

د. ب. ن:.....دون بلد نشر

ج:.....جزء

مج:.....مجلد

ط:.....طبعة

ع:.....عدد

ج:..... جريدة

ر:..... رسمية

ص:.....صفحة

ثانيًا- باللغة الفرنسية

CCF … .. .. ……... . . . . ……. . . . . Code Civile Français

CPF … . . . . . ……... . . . . …. Code Pénal Français

J.O…… Journal Officiel de la République Française

J.O.C.E…… Journal Officiel de Communautés Européennes

Cass.civ…….……...……..... Cour de Cassation Chambre Civil

Art: ……..…… Article

N ……. ……...……. …… . Numéro

P…….……..…...Page

Op.Cit…….……Ouvrage précédemment cité

Vol ……..…Volume

مقدمة

يتبين للمتمعن في تاريخ الكتابة أن الارتباط بينها وبين الورق ليس ارتباطا عضويا، وأن الكتابة باعتبارها ضربا من ضروب الرموز المتفق عليها في إطار اجتماعي معين قد ظهرت منذ عدة قرون قبل ظهور الورق، واتخذت لها عدة سندات مادية مثل جدران الكهوف والحجارة وجلود الحيوانات وخشب الأشجار، وفي خضم هذا التطوّر كان الورق آخر هذه السندات إلا أن تطوره وتدعيمه بأساليب الطباعة جعل من الفحوى المتمثل في الكتابة يرتبط ارتباطا وثيقا بشكله المادي الورقي إلى درجة التمازج والانصهار.

ومن الثابت أن الكتابة لا تعد دليلا كاملا في الإثبات إلا إذا كانت موّقعة، فالتوقيع يُعد بمثابة العنصر الثاني من عناصر الدليل الكتابي المعد للإثبات، باعتباره ينسب الورقة لمن وقعها. وبمعنى آخر الكتابة وحدها لا تعد دليلا كاملا في الإثبات ما لم تكن ممهورة بتوقيع يعد عنصرا ثانيا يكملها ويجعلها دليلا كاملا معدا للإثبات، وطالما أن التوقيع يمثل العنصر الثاني في الدليل الكتابي الكامل، فإن فقدان هذا العنصر يفقد هذا الدليل قوته الثبوتية.

إلى وقت ليس بالبعيد، كانت جل التعاملات القانونية تتسم بالوضوح والتحديد من حيث مضمونها، وكذلك من حيث طريقة إتمامها، ناهيك عن توفر قدر من الثقة والأمان فيها، والسبب يعود إلى أنها كانت تدون على محررات مادية، يمكن الوصول إليها والتأكد منها، أو من صحة التوقيع الذي يرد عليها، والوقوف على ما إذا كان مستوفيا لشروطه القانونية أم لا.

ظل هذا الوضع قائما إلى غاية التطور الذي شهده مجال تكنولوجيات المعلومات وقطاع الاتصالات، الذي كان له الأثر البالغ على المبادئ الراسخة في قواعد الإثبات. حيث أدى الاتصال والتعاقد عن بعد إلى شيوع استعمال المراسلات الإلكترونية، فلم تعد المراسلات والمحررات تقتصر على الدعامات التقليدية (الورقية) في تدوينها؛ بل أصبحت

تدون وتخزن على دعامات إلكترونية تعتمد على الشفرات والرموز؛ حيث لا يمكن الدخول إليها والاطلاع على مضمونها إلا بفك تشفيرها.

وفي ظل هذا الواقع التقني الجديد، الذي تتم فيه التعاملات والتصرفات القانونية عن بعد في صورة بيانات رقمية ومعلومات معالجة إلكترونيا، اختلف مفهوم المحرر المكتوب الذي تقوم عليه قواعد الإثبات بالكتابة، فلم يعد ضروريا أن يتخذ المحرر شكلا ورقيا، حيث ظهرت أنواع عديدة من المحررات تعتمد على دعامات غير ورقية أطلق عليها "**المحررات الإلكترونية**".

فضلا عن ذلك، تأثرت فكرة التوقيع كذلك نتيجة للتطور التقني، حيث لم يعد التوقيع التقليدي الطريقة الملائمة لتوثيق المعاملات الإلكترونية، ولتعذر استخدام التوقيع التقليدي على الدعامة الإلكترونية، ظهر بديل إلكتروني يتماشى مع الطبيعة التقنية لهذه الدعامة سُمي "**بالتوقيع الإلكتروني**"، يقوم على أشكال تكون في مجملها على شكل مجموعة من الرمـــــوز والأرقام والبيانات، ترتكز في الأساس على معادلات لوغاريتمية، على عكس التوقيع التقليدي الذي يقوم على البساطة في إنشائه ويكون في الغالب مقصورا على التوقيع بالإمضاء، الختم، وبصمة الإصبع.

إن ظهور المحررات الإلكترونية اللامادية إلى جانب المحررات التقليدية المادية، وظهور التوقيع الإلكتروني إلى جانب التوقيع العادي جعل المعاملات تتخذ شكلا إلكترونيا يمتاز بالتجريد واللامادية، بعيدا عن الواقع المادي الذي ظل مسيطرا على امتداد الأجيال السابقة، بحكم الاحتكام للمحررات الورقية الموقعة بأساليب التوقيع التقليدي، هذا ما جعل الفقه والقضاء يناديان بضرورة مواكبة هذه التغييرات تشريعيا، حيث سارعت العديد من الدول إلى وضع قوانين تنظم المعاملات الإلكترونية.

في ضوء ذلك، عرفت السنوات الأخيرة تدخلا تشريعيا واسعا على جميع المستويات؛ دوليا وإقليميا ووطنيا، إذ عملت العديد من المؤسسات الدولية على وضع نماذج قانونية لتدعيم الثقة في الأدلة الإلكترونية، ووضع القواعد الكفيلة بالاعتراف بقوتها

الثبوتية الكاملة. من هذه الجهود يأتي الدور الذي لعبته لجنة الأمم المتحدة، والتي حرصت على البحث في الإشكاليات والعقبات المتعلقة بقبول السندات الإلكترونية في الإثبات، وتَوّجت اللجنة أعمالها بإصدارها قانون نموذجي بشأن التجارة الإلكترونية عام (1996) الصادر بتاريخ (16 ديسمبر 1996) [1]، حيث احتوى على مجموعة من القواعد والإرشادات التي تهدف إلى تهيئة بيئة قانونية ملائمة للتجارة الإلكترونية، وكذا قبول الكتابة والتوقيع في الشكل الإلكتروني والاعتداد بهما من الناحية القانونية.

ثم أعقب ذلك بذل الكثير من الجهود الأوروبية التي تمخضت عن صدور التوجيه الأوروبي بشأن التوقيعات الإلكترونية رقم (93-1999) الصادر بتاريخ (12 ديسمبر 1999)[2]، والذي تضمّن مختلف المسائل القانونية والتقنية المتعلقة بالتوقيعات الإلكترونية، حيث كان يهدف إلى تسهيل عملية التوقيع الإلكتروني، وكذا المساهمة في الاعتراف بحجيته، وعلى العموم محاولة وضع إطار تنظيمي للتواقيع الإلكترونية وهيئات التصديق الإلكتروني.

وبعد حوالي سنتين تقريبا من صدور هذا التوجيه الأوروبي، أصدرت لجنة الأمم المتحدة للقانون التجاري في دورتها الرابعة والثلاثين، قانونا بشأن التوقيعات الإلكترونية لسنة (2001) الصادر بتاريخ (12 ديسمبر 2001) [3]، الغاية من ورائه ترسيخ فهم التوقيعات الإلكترونية وتعزيز الثقة بهذه التقنية الجديدة.

وبشكل عام؛ يهدف هذا القانون إلى مساعدة المشرع الوطني لدى الدول المنضوية تحت لواء الأمم المتحدة، إلى إقامة إطار قانوني لتنظيم التوقيعات الإلكترونية، فضلا عن إقراره مبدأ التكافؤ الوظيفي بين التوقيعات الإلكترونية والتوقيعات الخطية، وكذا مبدأ

---

(1)- قانون اليونسرال النموذجي بشأن التجارة الإلكترونية الصادر بقرار من الجمعية العامة للأمم المتحدة رقم 162/51 المؤرخ في 16 ديسمبر 1996، منشورات الأمم المتحدة، نيويورك، 2000، ص 1 إلى 13.

(2)- Voir la directive n° 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques, JO L 13 du 19.1.2000.
disponible sur site : http://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:31999L0093

(3)- قانون اليونسرال النموذجي بشأن التوقيعات الإلكترونية، الصادر بقرار من الجمعية العامة للأمم المتحدة رقم 80/56 المؤرخ في 12 ديسمبر 2001، منشورات الأمم المتحدة، نيويورك، 2002، ص 15 إلى 22.

الحياد التقني الذي يهدف إلى اتباع نهج مرن فيما يتعلق بالتقنيات المستخدمة في الكتابة أو التوقيع، وذلك بعد تفضيل تقنية معينة حتى ولو حققت درجة أكبر من الأمان والموثوقية.

بعد ذلك، أصدر المشرع الأوروبي التنظيم الأوروبي رقم (914-2014) الصادر عن البرلمان الأوروبي في (23 جويلية 2014)[1]، المتعلق بتحديد الهوية الإلكترونية وخدمات الثقة في المعاملات الإلكترونية داخل السوق الداخلي، والذي ألغى بموجبه التوجيه الأوروبي رقم (1999-93) سالف الذكر، وقد تضمن هذا التنظيم الأوروبي الجديد المبادئ نفسها التي اعترف بها التوجيه السابق الملغى، من حيث المساواة بين المحررات الإلكترونية والمحررات التقليدية في الإثبات طالما توافرت على الشروط القانونية المتعلقة بموثوقية التوقيع الإلكتروني وارتباطه بالمحرر الموقع به بشكل لا يقبل التعديل أو الانفصال، كما نظّم نشاط جهات التصديق الإلكتروني ومسؤولياتهم.

في الإطار نفسه، سارعت العديد من التشريعات الوطنية إلى التدخل لأجل تعديل القوانين الوطنية بما يتوافق مع المعطيات المستجدة المتعلقة بالتطور التقني والتكنولوجي؛ حيث صدرت قوانين تعنى بالمعاملات الإلكترونية التي أقرت من خلالها بحجية الدليل الكتابي في الإثبات، مكرسين بذلك مبدأ التكافؤ الوظيفي بين هذا الأخير وبين الدليل الكتابي التقليدي.

لم يكن المشرع الجزائري بمعزل عن التطورات الواقعة في هذا المجال، وإن كان تدخله قد جاء متأخرا جدا مقارنة بالدول العربية التي سبقته في ذلك، حيث تدخل المشرع الجزائري بداية بتعديله للقواعد العامة في الإثبات بدل اصدار قانون خاص بالمعاملات الإلكترونية، وهو ما كرسه من خلال تعديل قواعد الإثبات المنصوص عليها في القانون

(1)- Voir le règlement (UE) n° 910/2014 du parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/ce, journal officiel de l'union européenne L 257/73, 28/8/2014, disponible sur : https://eur-lex.europa.eu/legalcontent/FR/TXT/?uri=celex%3A32014R0910.

المدني، من خلال القانون (05-10) [1]، من خـــلال المادتين (323 مكـــرر1) و(327) منه، أين اعترف بالكتابة الإلكترونية والتوقيع الإلكترونـــــي؛ واعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة العادية، مع اشتراط إمكانية التأكّد من هوية الشخص الذي أصدرها من جهة، ومن جهة أخرى إعدادها في ظروف تضمن سلامتها.

ثم أصدر بعد ذلك المرسوم التنفيذي رقم (07-162) [2] المؤرخ في (30 ماي 2007) المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية، موضحا من خلاله بعض المسائل القانونية التقنية الخاصة بالتوقيع الإلكتروني، أين اعترف بالتوقيع والتوثيق الإلكتروني لكن لم يتبعه بإنشاء هيئات على أرض الواقع وترك هذه النصوص دون تجسيد.

ليصدر المشرع الجزائري بعد (08 سنوات) قانونا مستقلا خاصا بالتوقيع الإلكتروني؛ ألا وهو القانون رقم (15-04) المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين [3]، قام من خلاله بتنظيم الجوانب القانونية للاعتراف بحجية الكتابة والتوقيع في الشكل الإلكتروني وشروط ذلك، وتنظيم الجوانب المتعلقة بالتصديق الإلكتروني، ليصدر بعده المرسوم التنفيذي رقم (16-142) [4] المحدد لكيفيات حفظ الوثيقة الموقعة إلكترونيا، أين تطرق من خلاله لكيفيات حفظ الوثائق الإلكترونية.

---

(1)- أمر رقم 05-10 مؤرخ في 20 جوان 2005، ج.ر.ع 44، صادر في 26 جوان 2005، يعدل ويتمم الأمر رقم 75-58 المؤرخ في 26 سبتمبر 1975 المتضمن القانون المدني.

(2)- مرسوم تنفيذي رقم 07-162 مؤرخ في 30 ماي 2007، يتعلق بنظام الاستغلال المطبق على كل أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية، ج.ر. ع 37 صادر في 07 جويلية 2007، يعدل ويتمم المرسوم التنفيذي رقـــم 01- 123 مؤرخ في 09 ماي 2001، ج.ر.ع 27 صادر في 13 ماي 2007.

(3)- قانون رقم 15-04 مؤرخ في11 ربيع الثاني عام 1436 الموافق 01 فبراير سنة 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج.ر.ع 06، صادر في 10 فبراير 2015.

(4)- مرسوم تنفيذي رقم 16-142 مؤرخ في 27 رجب عام 1437 الموافق 5 مايو سنة 2016، يحدد كيفيات حفظ الوثيقة الموقعة إلكترونيا، ج. ر.ع 28 صادر بتاريخ 8 مايو سنة 2016.

من هنا، أثار موضوع "**النظام القانوني للإثبات الإلكتروني**"، رغبتنا للدراسة فيه، لنسعى من خلاله إلى بحث وتحليل القواعد القانونية المنظمة لمختلف جوانب الإثبات بالأدلة الإلكترونية المدنية والتجارية، وللحماية المقررة لها من أجل ضمان موثوقيتها في ظل التشريع الجزائري، رغبة منا في محاولة وضع بعض اللبنات التي تساهم في إرساء عناصر نظرية عامة تُعنى بالإثبات الإلكتروني أو على الأقل تبيان ما إذا كانت هناك فعلا نظرية عامة للإثبات الإلكتروني تتسم بالمرونة والقابلية للتعديل، مع تبيان أهم الثغرات القانونية التي وقع فيها المشرع الجزائري وإعطاء مختلف الحلول العملية لمختلف العقبات التي تواجه أدلة الإثبات الإلكتروني مستفيدين في ذلك من تجارب بعض التشريعات المقارنة.

تجدر الإشارة في هذا المقام أيضا إلى أننا قصرنا دراستنا على أدلة الإثبات الإلكتروني ذات الطابع المدني والتجاري دون غيرها، والتي نقصد بها على وجه الخصوص المحررات والتواقيع الإلكترونية، واستبعدنا الأدلة الإلكترونية الحديثة لإثبات غيرها من المعاملات الإلكترونية، كما استثنينا أدلة الإثبات الإلكتروني ذات الطابع الجنائي والإداري، لاختلافها عن أدلة الإثبات الإلكتروني ذات الطابع المدني والتجاري.

لدراسة الموضوع وتحقيق الهدف منه السابق تبيانه والمتمثل في محاولة وضع بعض اللبنات التي تساهم في إرساء عناصر نظرية عامة تُعنى بالإثبات الإلكتروني أو على الأقل تبيان ما إذا كانت هناك فعلا نظرية عامة للإثبات الإلكتروني تتسم بالمرونة والقابلية للتعديل، حاولنا الإجابة عن إشكالية **ما إن كان المشرع الجزائري ومن خلال الحجية القانونية التي منحها لأدلة الإثبات الإلكتروني مقارنة بأدلة الإثبات التقليدي قد وفّق في ذلك؟ وما إن كانت الضمانات التقنية والتشريعية المقررة لها كافية لتأمينها؟**

من خلال محاولتنا الإجابة عن هذه الإشكالية الرئيسية سنحاول الإجابة أيضا عن العديد من التساؤلات الفرعية التي تتمحور أساسا حول مفهوم الأدلة الكتابية المستحدثة؟ مدى إمكانية تطبيق النصوص القانونية العامة لتنظيمها؟ مدى الحاجة إلى استحداث

نصوص قانونية خاصة مستقلة عن الإثبات التقليدي؟ ماهي الآليات الكفيلة لحماية أدلة الإثبات الإلكتروني تدعيما للثقة في التعاملات الإلكترونية؟

إن طبيعة الموضوع والإشكالية المطروحة وكذا التساؤلات الفرعية تستدعي الاستعانة بأكثر من منهج، لذا إستعنا بكل من المنهج الوصفي والتحليلي لتناسبهما مع غرض الدراسة، وذلك من خلال وصف ودراسة المبادئ والأحكام التي تتعلق بالقواعد الخاصة بالإثبات الإلكتروني، والعمل على تحليلها لاستخلاص النتائج المترتبة عنها.

كما تم الاعتماد على المنهج المقارن من خلال التعرض في الكثير من الجزئيات إلى المقارنة بين العديد من القوانين الدولية منها والمحلية والتي تمثلت أساسا في كل من قانون اليونسترال والتنظيم الأوروبي باعتبارهما قوانين استرشادية، وكذا كل من القانون الفرنسي والمصري باعتبارهما مصدرين أساسين للقانون الجزائري، أما عن القانونين التونسي والمغربي فقد تم إدراجهما على اعتبار الوحدة الجغرافية التي تجمعهم بالجزائر. في حين تطرقنا للقانون الأردني على اعتبار أنه نظم قانون المعاملات الإلكترونية لمرتين سنة (2001) ليلغيه ويعيد تنظيمه بقانون جديد سنة (2015)؛ وذلك بغية الاطلاع على التجارب التشريعية المقارنة وحث المشرع الجزائري على الاستفادة منها.

للإجابة على إشكالية البحث وللوصول إلى تحقيق أهداف الدراسة، ارتأينا تقسيم الدراسة إلى بابين؛ تناولنا في الأول **أدلة الإثبات الإلكتروني** والذي تطرقنا من خلاله لكل من المحررات الإلكترونية والتوقيع الإلكتروني باعتبارهما أدلة الإثبات الإلكتروني، وبينا كلا من حجيتهما القانونية ومدى قبولهما في الإثبات.

في حين خصصنا الباب الثاني **للحماية المقررة لأدلة الإثبات الإلكتروني**، أين تطرقنا لأنواع الحماية المقررة لهذه الأدلة، والتي تمثّلت أساسا في الحماية التقنية والجزائية، وكذا بينا مدى كفايتها في تأمين أدلة الإثبات الإلكتروني.

الباب الأول

القيمة القانونية لأدلة الإثبات الإلكروني

الباب الأول
القيمة القانونية لأدلة الإثبات الإلكتروني

انتشرت وسائل الاتصال عن بعد وشاع التعامل عبر الوسائل الالكترونية وظهرت شبكة الانترنت كأحدث هذه الوسائل، خصوصا بعد البدء في استغلال هذه الشبكة في المجال التجاري، كما تم الشروع في استغلال هذه الشبكة في المجال الإداري في إطار ما يسمى بالحكومة الإلكترونية، بحيث أصبحت القطاعات العمومية والخاصة تقدم أغلب خدماتها عن طريق التبادل الالكتروني للمعطيات، معتمدة عليه –التبادل الإلكتروني للمعطيات– في اجراء المعاملات وابرام الصفقات، الشيء الذي نتج عنه ظهور العقود التي تبرم في الشكل الالكتروني كشكل جديد من أشكال التعاقد عن بعد.

لقد أثر هذا التطور الذي مس مجال تكنولوجيا المعلومات والاتصالات على المبادئ الراسخة في الفكر القانوني، خصوصا ما تعلق بعناصر الدليل الكتابي، فظهور وسائط حديثة لا مادية يمكن استخدامها في تدوين البيانات أثّر بشكل ملحوظ على عناصر الدليل الكتابي التقليدي التي لم تعد قادرة –العناصر– بمفردها على مجاراة التقدم الحاصل في مجال المعلوماتية، التي فصلت بين الرابطة التقليدية التي تجمع بين الكتابة والورق، فاتحة مجالا واسعا لمفهوم الكتابة، يرتكز بشكل خاص على اعتبارها رموزا معبرة عن الفكر، فأصبحت مجردة وغير مادية بخلاف الكتابة التقليدية، من جهة.

ومن جهة أخرى، لم يعد يشكل الورق في ظل هذا الواقع التقني سوى مجرد دعامة مادية للكتابة، يمكن أن تضاف لها دعامات أخرى طالما مكنّت الكتابة من أداء وظيفتها في الاثبات. وبذلك اختلف مفهوم المحرر التقليدي المكتوب الذي كانت تقوم عليه قواعد الإثبات بالكتابة، ليتحول من الشكل التقليدي المكتوب إلى شكل آخر إلكتروني قائم على دعامات لا مادية إلكترونية أطلق عليه مصطلح "المحرر الإلكتروني".

وفضلا عن ذلك، تأثرت فكرة التوقيع هي الأخرى، فلم يعد بالإمكان إصباغ توقيع تقليدي على محرر إلكتروني، ما دفع إلى ظهور نوع جديد من التوقيعات يتماشى مع طبيعة الدعامة

اللامادية للمحرر، كما يمكنه تأدية الوظائف نفسها التي يقوم بها التوقيع التقليدي، ويناسب في الوقت ذاته الركيزة الإلكترونية غير المادية، الأمر الذي أسفر عن إيجاد شكل جديد غير مألوف من التوقيعات، سُمي بـ: "التوقيع الإلكتروني"

وعليه يعتبر المحرر الموقع إلكترونيا المظهر الجديد للإثبات، غير أن الطبيعة اللامادية التي تقوم عليها كل من المحررات والتوقيعات الإلكترونية أثارت الكثير من الشكوك في قدرتها على أداء الوظائف ذاتها التي كانت تقوم بها كل المحررات والتوقيعات التقليدية، ونجم عن ذلك الكثير من الشكوك والتساؤلات حول مدى اعتبارها كأدلة كتابية؟ وإن كان في الإمكان إصباغ حجية قانونية عليها؟

وعلى اعتبار أن التعاملات التي تتم في بيئة إلكترونية صارت ضرورة حتمية فرضها التطور التقني الحاصل، سارعت العديد من التشريعات على المستويين الدولي والوطني إلى السعي نحو التنظيم القانوني للمحررات الإلكترونية **(فصل أول)**، وكذا التوقيعات الإلكترونية **(فصل ثان)**، واعتبارهما كأدلة إثبات إلكترونية. مع منح الحجية القانونية لكليهما، سواء بتطويع القواعد العامة للإثبات أو باستحداث قوانين ولوائح جديدة اعتمدت فيها كل من المحرر والتوقيع الإلكتروني ضمن طرق الإثبات.

الفصل الأول
المحررات الإلكترونية

كانت جل التعاملات القانونية إلى وقت ليس بالبعيد تتسم بالوضوح والتحديد من حيث مضمونها، وكذلك من ناحية طريقة إتمامها، ناهيك عن القدر المتوفر من الثقة والأمان فيها، ويعود السبب في ذلك إلى أنها كانت تدون على محررات ورقية مادية يمكن الرجوع إليها والتأكد منها في أي وقت وكلما استدعت الضرورة ذلك.

أما اليوم، فالعالم يعيش ثورة معلوماتية غير مسبوقة أحدثت تغييرات جذرية في العديد من المفاهيم القانونية السائدة، سواء على صعيد القانون العام أو الخاص، حيث ظهرت التعاملات الإلكترونية التي تعتمد على أسلوب غير ورقي، بل مرئي ومنقول عبر الشاشات الإلكترونية، لتُصبح المحررات الورقية لا تناسب هذا النوع من التعاملات الذي جرد المحررات والمعاملات من دعامتها المادية التقليدية وأحل محلها دعامات أخرى إلكترونية، أين تم استبدال الوثائق والملفات الورقية بالمحررات الإلكترونية.

تُعد المحررات الإلكترونية أسلوب أو وسيلة حديثة، تقوم بأداء وظائف المحررات الورقية فيما يتعلق بإثبات المعاملات؛ إذ تعتبر أحد أهم الأدوات لتحقيق فكرة الحكومة الإلكترونية التي تقدم خدماتها للأفراد والمؤسسات العامة والخاصة، كما تعتبر في الوقت ذاته وسيلة لتحقيق أهداف التجارة الإلكترونية؛ إذ يمكن بواسطتها إنجاز المعاملات وابرام الصفقات بكل سرعة وسهولة، وعليه تُعد المحررات الإلكترونية أسلوب أو وسيلة حديثة تقوم بأداء وظائف المحررات التقليدية فيما يتعلق بإثبات المعاملات، إلا أنها تختلف عنها نظرا للطبيعة التقنية التي تتميز بها نتيجة لقيامها في بيئة افتراضية لا مادية.

بعدما أصبحت المحررات الإلكترونية حقيقة قائمة لا يمكن تجاهلها في ابرام التصرفات القانونية، نجم عن ذلك ضرورة التدخل التشريعي لتنظيم جميع المسائل القانونية التي تعنى بتحديد الشروط القانونية والضوابط الفنية والتقنية الواجب توافرها في المحررات الإلكترونية،

وكذا تنظيم مسألة المساواة فيما بينها وبين المحررات التقليدية لأجل منحها الحجية القانونية في الإثبات حفاظا على استقرار المعاملات وحماية لحقوق الأفراد.

ولتوضيح ذلك ارتأينا التطرق إلى ماهية المحررات الإلكترونية باعتبارها أحد أدلة الإثبات الإلكتروني **(مبحث أول)**، ثم إلى الحجية المقررة لهذه المحررات الإلكترونية في الإثبات، وهل هي ذات الحجية المقررة للمحررات التقليدية باعتبار الأولى امتداد للثانية **(مبحث ثان)**.

المبحث الأول

ماهية المحررات الالكترونية

لقد أثرت التطورات التي مست مجال تكنولوجيا المعلومات والاتصالات على المبادئ الراسخة في الفكر القانوني، خصوصا ما تعلق بعناصر الدليل الكتابي. إن ظهور وسائط حديثة لا مادية يمكن استخدامها في تدوين البيانات أثّر بشكل ملحوظ على عناصر الدليل الكتابي التقليدي التي لم تعد قادرة بمفردها على مجاراة التقدم الحاصل في مجال تكنولوجيا المعلومات والاتصالات.

في ظل هذا الواقع التقني الجديد، الذي تتم فيه التصرفات القانونية عن بعد في صورة بيانات رقمية ومعلومات معالجة إلكترونيا، اختلف مفهوم المحرر المكتوب الذي تقوم عليه قواعد الاثبات بالكتابة، فلم يعد ضروريا أن يتخّذ المحرر شكلا ورقيا، بل ظهرت أنواع جديدة من المحررات تعتمد على دعامات غير ورقية وإنما إلكترونية يطلق عليها "المحررات الإلكترونية".

إن إدراك التشريعات الحديثة بحتمية التعامل بالمحررات الإلكترونية، وضرورة ضبط جوانبها القانونية لأجل توفير حماية وأمن للمتعاملين بها، دفعهم إلى معالجتها تشريعيا سواء بتطويع القواعد العامة للإثبات أو باستحداث قوانين ولوائح جديدة اعتمدت –ضمن طرق الإثبات– المحررات الإلكترونية التي تقوم على دعامات لا ورقية، وأسبغت عليها حجية كاملة في الإثبات شريطة أن تعد وتحفظ في ظروف من شأنها أن تضمن سلامتها.

لذا سنحاول من خلال هذا المبحث التطرق إلى مفهوم هذه المحررات الإلكترونية بناء على ما جاءت به تنظيمات الإثبات الإلكتروني سواء في القواعد القانونية العامة أو ما استحدثته بموجب نصوص خاصة **(مطلب أول)**، لنبين بعدها صور هذه المحررات الإلكترونية **(مطلب ثان)**.

المطلب الأول
مفهوم المحررات الالكترونية

اختلفت التشريعات الحديثة في إيجاد مصطلح مُوحد للمحرر الإلكتروني، لذا نجد العديد من المرادفات مثل "المستند الإلكتروني"، "الكتابة الإلكترونية"، "السجل الإلكتروني"، "رسالة البيانات"، "المحرر الإلكتروني"، وعلى الرغم من هذا الاختلاف إلا أن المعنى واحد، لأنه في الاصطلاح تؤخذ الألفاظ بمعناها العلمي المتفق عليه وليس بمدلولها اللفظي.

يقترن الاعتراف بالمحررات الإلكترونية بمبدأ مهم؛ ألا وهو مبدأ التعادل الوظيفي فيما بينها وبين المحررات الورقية التقليدية، وتظهر أهمية هذا المبدأ في أنه يضفي على المحررات الإلكترونية الحجية ذاتها المقررة للمحررات الورقية، ويتم الاعتراف بالمحرر الإلكتروني كدليل كتابي في سياق بيان مفهومه الذي جاء بها كل من الفقه والتشريع **(فرع أول)**، وكذلك فيما يخص تحديد عناصر قيامه وشروطه التي تضمن أداء وظائف المحرر التقليدي **(فرع ثان)**.

الفرع الأول
التعريف بالمحررات الالكترونية في الفقه والتشريع

فرضت المحررات الإلكترونية نفسها في التعامل وأصبحت واقعا لا يمكن إنكاره، وامتدت لتشمل سائر فروع القانون؛ العام والخاص على حد سواء؛ لذلك عمل كل من الفقه والتشريع الدولي والوطني على إعطاء مفاهيم متنوعة للمحررات الإلكترونية تتسم بالمرونة لاستيعاب مستجدات التقدم التقني، وهو ما دفعنا إلى أن نورد كل من مساهمة الفقه **(أولا)**، والتشريع الدولي **(ثانيا)**، والتشريعات الوطنية **(ثالثا)**، في محاولة تحديد مفاهيم دقيقة للمحررات الإلكترونية.

أولا: التعريف الفقهي للمحررات الإلكترونية

اهتم الفقه بشكل كبير بتعريف المحررات الإلكترونية باعتبارها وسيلة إثبات حديثة، من هذا المنطلق عرّف جانب من الفقه المحرر الإلكتروني بأنه: « **القيد أو العقد الذي يتم إنشاؤه عن طريق استخدام تقنية كهربائية أو مغناطيسية أو ضوئية أو كهرومغناطيسية أو أي وسيلة مشابهة، بحيث لا يتوفر به عنصر الكتابة التقليدية أو الورقة العادية أو التوقيع العادي فيلجأ في إنشائه إلى أساليب حديثة إلكترونية عن طريق تدوينه برموز خاصة على دعامة إلكترونية أو رقائق، ويتم التوقيع عليه أيضا بطريقة إلكترونية وليس تقليدية مع احتمال تعرضه لمخاطر التغيير والتبديل أو التلف والفقدان بصورة أكبر من المحرر العادي**»[1].

ويرى جانب آخر من الفقه أن أفضل تعريف فقهي للمحرر الإلكتروني هو: «**كل بيان على شكل كتابة أو صورة أو صوت يتم إنشاؤه أو إرساله أو تسلمه أو خزنه أو تجهيزه بوسائل إلكترونية**»[2].

وعرفت أيضا بأنها: «**مجمع بيانات أو معلومات يتم تبادلها بوسائل الكترونية كشبكة الإنترنت وأية وسيلة أخرى مشابهة، تعطي دلالة قابلة للإدراك**»[3].

ولأجل إعطاء قيمة قانونية للمحرر الإلكتروني وجب ارتباطه بتوقيع إلكتروني، ليعرف على أنه: «**معلومات يتم إنشاؤها أو إرسالها أو تخزينها أو استلامها بوسيلة إلكترونية أو ضوئية أو رقمية أو صوتية مادام تتضمن إثبات واقعة أو تصرف قانوني محدد وتتضمن توقيع إلكتروني ينسب هذه الواقعة أو التصرف لشخص محدد**»[4].

---

(1) – يوسف أحمد النوافلة، حجية المحررات الالكترونية في الإثبات، ط1، دار وائل للطباعة والنشر، الأردن، 2007، ص 54؛ أنظر أيضا **محمد فواز المطالقة**، الوجيز في عقود التجارة الالكترونية (أركانها – إثباتها – حمايتها – التوقيع الالكتروني – القانون الواجب التطبيق)، دار الثقافة للنشر والتوزيع، الأردن، 2008، ص 205.

(2) – عباس العبودي، التعاقد بوسائل الاتصال الفوري، وحجيتها في الإثبات، دار الثقافة، الأردن، 1997، ص 37.

(3) – محمد محروك، مظاهر التقاطع والتكامل بين المحررات العادية والمحررات الالكترونية وفق القواعد العامة والقانون 05-53، مجلة الأملاك، مجلة فصلية تعنى بالدراسات القانونية والفقهية، المغرب، العدد المزدوج 6، 2009، ص 113.

(4) – محمد أمين الرومي، المستند الالكتروني، دار الكتب القانونية، مصر، 2008، ص 55.

ثانيا: تعريف المحررات الالكترونية في التشريع الدولي

تطرقت أكثر من منظمة ولجنة دولية لتعريف المحررات الإلكترونية من خلال قوانين التجارة الإلكترونية، وأهم منظمتين تطرقتا بإسهاب لموضوع المحررات الإلكترونية، هما منظمة الأمم المتحدة عن طريق لجنتها للقانون التجاري الدولي- اليونسترال- والاتحاد الأوربي كمنظمة إقليمية.

أ/ في قانون اليونسترال بشأن التجارة الإلكترونية:

يعتبر قانون اليونسترال النموذجي بشأن التجارة الإلكترونية لسنة (1996) [1] أول نص تشريعي يقر عدم التمييز والحياد التكنولوجي والتكافؤ الوظيفي بين المحررات التقليدية والمحررات الإلكترونية، حيث يعتبره الكثيرون أنه أساس قانون التجارة والمعاملات الإلكترونية الحديثة، وبالرجوع للمادة (5) منه نجدها تنص على أنه: «**لا تفقد المعلومات مفعولها أو صحتها أو قابليتها للتنفيذ لمجرد أنها في شكل رسالة بيانات**»، وبالرجوع لنص المادة (2- أ) من القانون نفسه نجده قد عرف المحرر الالكتروني مطلقة عليه مصطلح رسالة البيانات وهي:« **المعلومات التي يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها بوسائل إلكترونية أو ضوئية أو بوسائل مشابهة، بما في ذلك على سبيل المثال لا الحصر تبادل البيانات الإلكترونية، أو البريد الإلكتروني، أو البرق، أو التلكس، أو النسخ البرقي**».

---

(1) - اليونسترال (unicitral) اختصار لمسمى **United nation commission for International Trade Law** وهي لجنة الأمم المتحدة للقانون التجاري الدولي، أنشأت عام 1966، بموجب قرار هيئة الأمم المتحدة رقم (2205/ د – 21) بتاريخ 17 ديسمبر 1966، عُهد إليها بتطوير القواعد المتعلقة بالأعمال التجارية الدولية وسن القوانين النموذجية، تعتبر قوانينها استرشادية للدول، إذ يمكن لهذه الأخيرة العودة لقوانين اليونسترال حين تنظيمها لقوانينها؛ فهو قانون إطاري مرجعي كما ورد في الدليل التشريعي الخاص بها.

- القانون النموذجي بشأن التجارة الالكترونية المعتمد من طرف لجنة الأمم المتحدة للقانون التجاري الدولي في الجلسة العامة رقم 85 في 6 كانون الأول/ ديسمبر 1996، والقانون النموذجي بشأن التوقيعات الالكترونية الذي اعتمدته ذات اللجنة بناء على القرار رقم 80/56 في جلستها العامة 85 في 12 كانون الأول / ديسمبر 2001. أنظر الموقع http://www.uncitral.org

ما نستنتجه من المادة (2– أ) أعلاه، أنها أعطت رسالة البيانات نفس القيمة مهما كانت الوسيلة المستخدمة إلكترونية أو ضوئية، أو أية وسيلة مشابهة. كذلك عبارة على سبيل المثال لا الحصر، فتحت المجال لما قد تنتجه لنا الحضارة مستقبلا، وذلك لاعتمادها مبدأ الحياد التقني.

ب/ في إطار التوصيات الأوروبية:

لم يُعرف التوجيه الأوروبي (93/99) الصادر في (12 ديسمبر 1999) بشأن التوقيع الالكتروني المحرر الالكتروني، وإنما اقر مبدأ التكافؤ الوظيفي بين المحرر الإلكتروني والعادي، حيث ساوى بينهما من حيث القيمة والحجية في الإثبات، طالما توفرت في المحرر الالكتروني كل من شرط الاستمرارية، عدم القابلية للتعديل، وارتباط التوقيع بالمحرر على نحو لا يقبل الانفصال، وكذا شرط اعتماده بشهادة متخصصة [1]، كما أن التوجيه الأوروبي (31/2000) المؤرخ في (08 جوان 2000) المتعلق بالتجارة الإلكتروني[2] ، لم يعط تعريفا للمحرر الإلكتروني وإنما حث على تسهيل إبرام العقود في الشكل الإلكتروني.

ثالثا: تعريف المحررات الإلكترونية في بعض التشريعات الوطنية المقارنة

عدلت الكثير من التشريعات الوطنية أحكام قوانينها حتى تلائم التطور التقني الذي مس وسائل الاتصال الحديثة لتشمل بذلك فكرة المحرر الإلكتروني، في حين أصدرت دول أخرى قوانين خاصة لتنظيم المعاملات الإلكترونية، وقد ارتأينا التطرق بالدراسة لكل من القانونين الفرنسي والمصري لتشابه تنظيمهما مع القانون الجزائري، كما درسنا كل من القانون التونسي والمغربي باعتبارهما دول المغرب العربي، في حين تطرقنا للتشريع الأردني على اعتبار أنه نظم قانون المعاملات الإلكترونية لمرتين سنة (2001) ليلغيه ويعيد تنظيمه بقانون جديد سنة (2015).

(1) - Article 02 du le directive Européenne 99/93 du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques.

(2) - Considération de parlement Européen sur la directive 2000/31 du 08 juin 2000 sur le commerce électronique**.** https://www.legifrance.gouv.fr

أقر المشرع الفرنسي تعديلات هامة على قانون الإثبات الفرنسي القديم، وذلك من خلال القانون رقم (230 لسنة 2000) الصادر بتاريخ (13-03-2000) المتعلق بالإثبات الإلكتروني والتوقيع الإلكتروني[1]، أين اعترف بالحجية القانونية للمحررات الإلكترونية مساويا بذلك بينها وبين المحررات الورقية[2]، حيث ورد في نص المادة (1316) المعدلة: «**الإثبات الخطي، الإثبات بالكتابة ينتج من كل تدوين للحروف أو العلامات أو الأرقام أو أي رموز أو إشارات ذات دلالة تعبيرية مفهومة وواضحة، أيا ما كـــانت دعامتـــها أو وسـيلة نقلها**»[3]، وبالتالي وسع من مفهوم المحرر المكتوب ليشمل الكتابة العادية والإلكترونية.

ليقم بعد ذلك المشرع الفرنسي بتعديل القانون المدني بموجب الأمر رقم (2016-131) الصادر بتاريخ (10 فيفري 2016) بشأن إصلاح قانون العقود وإثبات الالتزامات [4]، لينص من خلال المادة (1365) منه على أن: «**الكتابة تتكون من سلسلة من الحروف أو الأشكال أو الأرقام أو أي إشارات أو رموز تعطي دلالة مفهومة، أيا كانت الدعامة المثبتة عليها**».

يتضح من خلال هذا التعريف أن المشرع الفرنسي لم يُعرف المحرر الإلكتروني، وإنما وسّع من تعريف الكتابة لينصرف لمفهوم الكتابة العادية على دعامة ورقية وكذلك الكتابة المثبتة على دعامة إلكترونية، من خلال استخدامه لعبارة " أيا كانت الدعامة"، ليواكب بذلك أي تطور تكنولوجي قد يظهر مستقبلا.

)-1(Loi n° 2000-230 du 13 Mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, J. O ,du 14 Mars 2000, p 3968, J.C.P.2000 ,III , 20259.
https://www.legifrance.gouv.fr/

(2) – محمد محمد سادات، حجية المحررات الموقعة إلكترونيا في الإثبات – دراسة مقارنة –دار الجامعة الجديدة، مصر، 2011، ص 81؛ أنظر كذلك **ناصر حمودي**، العقد الدولي الإلكتروني المبرم عبر الانترنت مع التركيز على عقد البيع الدولي للبضائع، دار الثقافة للنشر والتوزيع، الأردن، 2012، ص 250؛ وأنظر أيضا:

CAPRIOLI (E. A), Signature électronique, La loi Français sur la preuve et la signature électronique dans la perspective Européenne, dire 1999/93, j c p. La semaine juridique, édition général n : 18,03 mai 2000 p 787.
https://www.caprioli-avocats.com/

)-3(Article (1316 Loi n° 2000-230 du 13 Mars 2000): «**La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission».**

)-4(Ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations, JORF n°0035 du 11 février 2016texte n° 26.
https://www.legifrance.gouv.fr/

أما عن المشرع التونسي فقد سبق نظراءه العرب في مجال تقنين المعاملات الإلكترونية بإصداره قانون المبادلات والتجارة الإلكترونية سنة (2000) [1]، لكنه لم يعرف من خلال هذا القانون المحررات الإلكترونية، إلا أنه من خلال نص المادة (453 مكرر) من مجلة الالتزامات والحقوق، والتي أضيفت بموجب القانون (57 لسنة 2000) المؤرخ في (13 جوان 2000) عرّف الوثيقة الإلكترونية بأنها: « **الوثيقة المكونة من مجموعة أحرف وأرقام أو إشارات رقمية أخرى بما في ذلك تلك المتبادلة عبر وسائل الاتصال تكون ذات محتوى يمكن فهمه ومحفوظة على حامل إلكتروني يؤمن قراءتها والرجوع إليها عند الحاجة** »، وقد اعترف المشرع التونسي من خلال الفقرة الثانية من هذه المادة بالحجية للوثيقة الإلكترونية وذلك بنصه أن الوثيقة الإلكترونية:« **تعد كتابا غير رسمي إذا كانت محفوظة في شكلها النهائي بطريقة موثوق بها ومدعمة بإمضاء إلكتروني**».

نلاحظ من خلال هذه النصوص أن المشرع التونسي عبر عن المحرر الإلكتروني بمصطلح الوثيقة الإلكترونية، والتي اعتبر أنها مجموعة أحرف، أو أرقام، أو أي إشارات رقمية أخرى، فاتحا المجال لاستيعاب ما قد يبتكر مستقبلا من تقنية لإنشائها وبذلك فقد سلك مسلك قانون اليونسترال النموذجي المتعلق بالتجارة الإلكترونية لسنة (1996).

في حين لم يعرف المشرع المغربي صراحة الوثيقة الإلكترونية أو المحرر الإلكتروني من خلال القانون رقم (05-53)[2] المتعلق بالتبادل الإلكتروني للمعطيات القانونية وذلك بخلاف القانون التونسي، إلا أنه أعطى مفهوم حديث للكتابة، حيث أدخلت المادة الخامسة منه تغييرا على نص المادة (417) من قانون الالتزامات والعقود، وذلك على الشكل التالي: «**الدليل**

---

(1)- القانون التونسي رقم 83 لسنة 2000، مؤرخ في 09 ماي 2000، المتعلق بالمبادلات والتجارة الإلكترونية، منشور في الرائد الرسمي للجمهورية التونسية، العدد 64، الصادر في 11 أوت 2000. http://www.legislation.tn

(2)- ظهير شريف رقم 129.07.1 صادر في 30 نوفمبر 2007 بتنفيذ القانون رقم 05-53 المتعلق بالتبادل الإلكتروني للمعطيات القانونية، منشور في الجريدة الرسمية عدد 5584 بتاريخ 06 ديسمبر 2007. https://adala.justice.gov.ma/

الكتابي ينتج من ورقة... أو رموز أخرى ذات دلالة واضحة، كيفما كانت دعامتها وطريقة إرسالها»[1].

يتضح لنا أن المشرع المغربي اعترف بالكتابة الإلكترونية وأقر إمكانية قيام الدليل الكتابي انطلاقا من وثيقة إلكترونية، وأدرج كذلك إمكانية أن يكون الدليل الكتابي محمولا على دعامة ورقية أو على دعامة إلكترونية، كما أن طريقة تبادله لم يعد لها دور مؤثر، إذ يمكن تبادله عن طريق التسليم المباشر أو بالمراسلة أو بشكل إلكتروني.

بينما عرّف المشرع المصري وفقا لنص المادة (1/أ) من قانون التوقيع الإلكتروني المصري رقم (15 لسنة 2004) [2] الكتابة الإلكترونية بأنها: «**كل حروف وأرقام أو رموز أو أي علامات أخرى تثبت على دعامة الإلكترونية أو رقمية أو ضوئية أو أية وسيلة أخرى مشابهة وتعطي دلالة قابلة للإدراك**»، كما عرّف المحرر الإلكتروني في المادة (1/ب) بأنه: «**رسالة بيانات تتضمن معلومات تنشأ أو تدمج، أو تخزن أو ترسل أو تستقبل كليا أو جزئيا بوسيلة إلكترونية أو رقمية أو ضوئية أو بأي وسيلة أخرى مشابهة**».

فرّق بذلك المشرع المصري –من خلال هذين النصين– بين الكتابة الإلكترونية والمحرر الإلكتروني حتى يزيل أوجه الخلط بينهما، كما أنه أعطى مجالا واسعا للمحرر الإلكتروني بحيث لم يقتصر على المحررات التي يتم تداولها عبر شبكة الإنترنت، بل أجاز كذلك استخدام وسائل إلكترونية أخرى كإمكانية استخدام الفاكس أو التلكس أو أي وسيلة تتاح مستقبلا[3].

أما عن المشرع الأردني فقد مر الاعتراف بالمحررات الإلكترونية بالعديد من المراحل، حيث قام المشرع الأردني بتنظيم هذا النوع من المحررات في بعض القطاعات الحيوية

---

(1) – مشار له لدى: **عبد الحكيم زروق**، التنظيم القانوني للمغرب الرقمي، ط1، مكتبة الرشاد، المغرب، 2013، ص 26.

(2) – قانون التوقيع الإلكتروني المصري 15 لسنة 2004، صادر في 21 أفريل 2004، جريدة رسمية عدد 217، بتاريخ 22 -04- 2004. https://elpai.idsc.gov.eg/

(3) – **مليكة مراد**، طرق الإثبات الإلكترونية المدنية، أطروحة لنيل شهادة الدكتوراه في الحقوق، كلية الحقوق، جامعة أمحمد بوقره، بومرداس، 2018 ص 24.

للمملكة [1]. ثم في مجال المعاملات الإلكترونية بموجب القانون (85 لسنة 2001) [2]، حيث عرفت المادة الثانية منه "المحرر الإلكتروني" بأنه: «**المعلـومات التي يتم انشـــاؤها، أو إرسالها، أو استلامها أو تخزينها بوسائل إلكترونية أو وسائل مشابهة بما في ذلك على سبيل المثال لا الحصر تبادل البيانات الإلكتروني والبريد الإلكتروني أو البـــرق أو التلكس أو النسخ البرقي**»، وعرّف السجل الإلكتروني بأنه: «**رســـالة البيانـــات أو القيد أو العقد أو المعلومات التي أنشأت أو أرسلت أو خزنت بوسائل إلكترونية**».

نلاحظ أن المشرع الأردني من خلال القانون رقم (85 لسنة 2001) قد تبنى تعريف لجنة اليونسترال للمحررات الإلكترونية، وقد أقر كذلك حجية المحرر الإلكتروني من خلال نص المادة (9) من القانون نفسه بنصه على أنه: «**إذا اتفق الأطراف على إجراء معاملة بوسائل إلكترونية وكانت التشريعات تتطلب ابراز المعلومات أو إرسالها أو تسليمها بوسائل إلكترونية يفي بمتطلبات تلك التشريعات، إذا كان المرسل إليه قادر على طباعة تلك المعلومات وتخزينها والرجوع إليها في وقت لاحق بالوسائل المتوفرة لديه**».

مما سبق؛ نستنتج أن المشرع الأردني أضفى شرطا وحيدا حتى تتمتع المحررات الإلكترونية بالحجية القانونية، ألا وهو قدرة المرسل إليه على طباعة المعلومات وتخزينها والرجوع إليها لاحقا بالوسائل المتوفرة لديه.

---

(1) – تناول المشرع الأردني مسألة الإثبات الإلكتروني في المادة (72 – 6) من قانون الأوراق المالية المؤقت لسنة (1997) بنصها: « **يجوز الإثبات في قضايا الأوراق المالية بجميع طرق الإثبات بما في ذلك البيانات الإلكترونية أو الصادرة عن الحاسوب وتسجيلات الهاتف ومراسلات أجهزة التلكس والفاكسميل** »، وكذلك في قانون براءة الاختراع، وكذا قانون الرسوم والنماذج الصناعية لسنة (2000)، وفي قانون أصول المحاكمات المدنية حيث تنص المادة(80 /01) منه على أن: « **يدون كاتب الضبط محضر المحاكمة بخط اليد أو بواسطة أجهزة الحاسوب أو الأجهزة الإلكترونية** »؛ أنظر في ذلك: **ناصر حمودي**، مرجع سابق ص 256؛ **مراد طنجاوي**، مرجع سابق، ص 55.

(2)– القانون (85 لسنة 2001) المتعلق بالمعاملات الإلكترونية الأردني الملغى، منشور بالجريدة الرسمية للمملكة الأردنية الهاشمية، عدد 4542، الصادر بتاريخ 2001/12/31. https://lob.gov.jo/

كما أصدر المشرع الأردني قانونا جديدا للمعاملات الإلكترونية سنة (2015) ألا وهو القانون (15 لسنة 2015) المتعلق بالمعاملات الإلكترونية الأردني [1]، حيث أعاد صياغة تعريف المحررات الإلكترونية بنصه من خلال المادة (2) منه على أن رسالة المعلومات الإلكترونية هي: « **المعلومات التي يتم إنشاؤها أو إرسالها أو تسلمها أو تخزينها بأي وسيلة إلكترونية ومنها البريد الإلكتروني أو أي تبادل للمعلومات إلكترونيا**»، في حين عرّف السجل الإلكتروني بأنه: « **رسالة المعلومات التي تحتوي على قيد أو عقد أو أي مستند أو وثيقة من نوع آخر يتم إنشاء أي منها أو تخزينها أو استخدامها أو نسخها أو إرسالها أو تبليغها أو تسلمها باستخدام الوسيط الإلكتروني** ».

نلاحظ من خلال هذه التعريفات، أن المشرع الأردني أعطى وصف رسالة المعلومات على المحرر الإلكتروني واعتبره مجموعة من المعلومات التي تنشأ أو ترسل أو تسلّم أو تخزّن بأي وسيلة إلكترونية، هاته الأخيرة التي ذكرها على سبيل المثال لا الحصر فاتحا المجال بذلك لما قد يبتكر مستقبلا.

كما نلاحظ كذلك، أن المشرع الأردني قد حدد نطاق كل من السجل الإلكتروني ورسالة المعلومات، فوسّع من نطاق هذه الأخيرة لتشمل الأولى. ومنه فإن كل سجل إلكتروني يعتبر رسالة معلومات وليس العكس؛ موسّعا بذلك من نطاق رسالة المعلومات.

أما بالنسبة للمشرع الجزائري فقد تبنى الاتجاه نفسه الذي سـار عليه المشـرع الفرنسـي، فهو لم يعط تعريفا للمحرر الإلكتروني وإنما وسع من مفهوم الكتابة لتشمل الكتابة العادية والكتابة الإلكترونية؛ وذلك من خلال تعديله لأحكام القانون المدني المتعلقة بالإثبات[2]، حيث نص في المادة (323) من القانون المدني الجزائري على: «**ينتج الإثبات بالكتابة من**

---

(1)– القانون 15 لسنة 2015 المتعلق بالمعاملات الإلكترونية الأردني، منشور بالجريدة الرسمية للمملكة الأردنية الهاشمية، عدد 5341، الصادر بتاريخ 2015/05/17. https://lob.gov.jo/

(2) – القانون رقم 05 – 10 مؤرخ في 13 جمادى الأولى 1426 الموافق 20 يونيو 2005 يعدل ويتمم الأمر رقم 58/75 مؤرخ في 20 رمضان 1395 الموافق 26 سبتمبر 1975 المتضمن القانون المدني، ج ر ع 44، صادر في 26 يونيو 2005.

تسلسل حروف أو أوصاف أو أرقام أو أية علامات أو رموز ذات معنى مفهوم، مهما كانت الوسيلة التي تتضمنها، وكذا طرق إرسالها».

من خلال استقرائنا لنص هذه المادة، نجد أن المشرع الجزائري لم يميز بين الدعامات التي تتضمن الكتابة، سواء كانت عادية أو إلكترونية أو أي دعامة قد تظهر مستقبلا ما دامت الكتابة ذات معنى مفهوم.

كما أنه من خلال نص المادة (323 مكرر 1) ساوى بين الحجية المقررة للكتابة على الورق والحجية المقررة للكتابة الإلكترونية [1].

لم ينص القانون (15- 04) المتعلق بالقواعد العامة للتوقيع والتصديق الإلكترونيين سالف الذكر، على أي تعريف للمحرر الإلكتروني إلا أنه ذكر مصطلح وثيقة إلكترونية في المادة 04 منه: «**تحفظ الوثيقة الموقعة إلكترونيا في شكلها الأصلي، ويتم تحديد الكيفيات المتعلقة بحفظ الوثيقة الموقعة إلكترونيا عن طريق التنظيم**»، ثم من خلال المرسوم التنفيذي رقم (16- 142) الذي يحدد كيفيات حفظ الوثيقة الموقعة إلكترونيا[2]، عرّف الوثيقة الإلكترونية في المادة (2) فقرة (1) منه: «**مجموعة تتألف من محتوى وبنية منطقية وسمات العرض، تسمح بتمثيلها واستغلالـــها من قبل الشخص عبر نظـــام إلكترونـــي**»، وعرّف الوثيقة الموّقعة إلكترونيا في المادة نفسها بأنها: «**وثيقة إلكترونية مرفقة أو متصلة بتوقيع إلكتروني**».

لقد جاء هذا التعريف غير دقيق ولا يمكن من خلاله تحديد شكل معين للمحرر أو الوثيقة الإلكترونية، على عكس ما جاءت به التشريعات السابقة الذكر أعلاه.

من كل ما سبق يمكننا تعريف المحرر الإلكتروني بأنه عبارة عن بيانات مكتوبة في شكل إلكتروني قابلة للإدراك، تنشأ أو تخزن أو ترسل أو تستلم باستخدام نظام المعالجة الآلية

---

(1) – تنص المادة (323 مكرر 1) على أنه: «**يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق، بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها**».

(2) – مرسوم تنفيذي رقم (16 – 142) مؤرخ في 27 رجب عام 1437 الموافق 05 مايو سنة 2016، يحدد كيفيات حفظ الوثيقة الموقعة إلكترونيا، ج ر ع 28 صادر في 08 مايو 2016.

للمعطيات، تعبر عن إرادة صاحبها، ومحفوظة ضمن ظروف تضمن سلامتها للرجوع إليها عند الحاجة.

الفرع الثاني
محددات المحرر الإلكتروني

لإنشاء تصور كامل عن المحرر الإلكتروني لابد من التطرق لبعض النقاط الضرورية، حيث من خلالها يمكننا تحديد مفهوم شامل عن المحرر الإلكتروني باعتباره دليل كتابي يُعتد به في الاثبات. تتمثل هذه النقاط أساسا في عناصر المحرر الإلكتروني التي يقوم عليها، وهل هي ذاتها عناصر المحرر التقليدي؟ **(أولا)**، وتحديد شروط صحته التي إذا ما توافرت حقق المحرر الإلكتروني ذات الوظائف المقررة للمحرر التقليدي **(ثانيا)**.

أولا: عناصر المحرر الإلكتروني

تقوم المحررات التقليدية على وجود دعامة ورقية تحتوي على كتابة خطية ممهورة بتوقيع صاحبها حتى يُعتد بها في الإثبات، في مقابل ذلك وحتى تكون للمحررات إلكترونية حجية في الإثبات شأنها في ذلك شأن المحررات التقليدية المعدة للإثبات، لا بد من توافر دعامة إلكترونية تحتوي على كتابة وتوقيع إلكترونيين مستوفيان لشروطهما.

نستنتج مما تقدم؛ أن المحرر الإلكتروني الذي يصلح ليكون بديلا للمحرر التقليدي في إثبات التصرفات القانونية المبرمة عبر وسائل الاتصال الحديثة، لابد أن يقوم على عنصرين أساسين لا يكتمل إلا بهما؛ وهما الكتابة الإلكترونية والتوقيع الإلكتروني؛ وهذا ما سنقوم بتفصيله في النقطتين المواليتين.

1- الكتابة الإلكترونية:

تم التخلي عن المفهـــوم الضيّق للكتابـــة والتي كانت تتم يدويا أو بواسطـــة الآلة الكاتبة نتيجة للتطور المستمر في الوسائل الحديثة التي يتم من خلالها إجراء التصرفـــات القانونية، فظهرت الكتابة الإلكترونية وهي تلك التي يتم إدراجها على دعائم إلكترونية قابلة

للاسترجاع أو الاستنساخ بواسطة جهاز الحاسوب، أو أي تقنية أخرى مهما كان نوعها أو درجة تقدمها أو مكوناتها المادية. وبهذا تختلف الكتابة الإلكترونية عن الكتابة التقليدية من حيث وسيلة إعدادها والتي تكون إلكترونية، إلا أن الغاية التي ينشآن من أجلـــها واحـــدة، ألا وهي التعبير عن فكرة معينة يراد إظهارها إلى حيز الوجود [1].

اهتم الفقه وبعض التشريعات المقارنة بوضع تعريف للكتابة الإلكترونية باعتبارها أحد عناصر المحرر الإلكتروني، وسنحاول توضيح ذلك فيما يلي من خلال التطرق لكل من التعريف الفقهي للكتابة الإلكترونية، وكذا التعريفات التي أقرتها التشريعات المقارنة لهذه الأخيرة.

أ- التعريف الفقهي للكتابة الإلكترونية:

تعرّف الكتابة الإلكترونية على أنها: «**المعلومات التي تسجل أو توضع على وسائط إلكترونية ويكون تخزينها دائم أو لفترة يعد فيها المحرر صالحا للاستعمال**» [2]، وعرفت أيضا بأنها: «**كل حروف أو أشكال أو أرقام أو رموز أو إشارات أو أي علامات أخرى ذات دلالة قابلة للإدراك أيا كانت الدعامة المثبتة عليها، إلكترونية أو رقمية أو ضوئية أو أية وسيلة أخرى مشابهة**» [3].

ويمكننا تعريف الكتابة الإلكترونية بأنها مجموعة من الأرقام أو الإشارات أو الأحرف أو الرموز الأخرى ذات دلالة واضحة، أيا كانت ركيزتها، إلكترونية أو رقمية أو ضوئية أو أية وسيلة أخرى مشابهة.

ب- تعريف الكتابة في التشريعات المقارنة:

---

(1)- نائل علي مساعدة، الكتابة في العقود الإلكترونية في القانون الأردني، مجلة الشريعة والقانون، كلية القانون، جامعة الإمارات العربية المتحدة، العدد 50، السنة 26، أفريل 2012، ص 201.

(2)- حسن فضالة موسى، التنظيم القانوني للإثبات الإلكتروني، مكتبة السنهوري، لبنان، ط1، 2016، ص 88.

(3)- جمال عبد الرحمن محمد علي، الحجية القانونية للمستندات الإلكترونية، دار الكتب، مصر، 2004، ص09.

نظمّت التشريعات الحديثة الإطار القانوني للكتابة الإلكترونية، فمنها من قامت بتنظيمه بموجب نصوص خاصة مستقلة عن قواعد الإثبات التي ينظمها القانون المدني، مثل التشريع المصري والأردني.... في حين فضّلت بعض التشريعات الأخرى على أن تعدّل قانونها المدني بإضافة هذا المصطلح الحديث مثل، فرنسا، الجزائر، تونس، المغرب.

ما يلاحظ على هذه التشريعات اختلافها في تسمية الكتابة الإلكترونية؛ حيث أطلق عليها قانون اليونسترال النموذجي مصلح "رسالة البيانات"، في حين استعمل المشرع المصري مصطلح "الكتابة الإلكترونية"، بينما استخدم المشرع الفرنسي والجزائري مصطلح "الكتابة المتخذة شكلا إلكترونيا" [1].

نجد المشرع المصري قد عرّف الكتابة الإلكترونية بموجب نص المادة (1/أ) من قانون التوقيع الإلكتروني لسنة (2004) بأنها: «**كل حروف أو أرقام أو رموز أو أي علامات أخرى تثبت على دعامة إلكترونية أو رقمية أو ضوئية أو أية وسيلة أخرى مشابهة وتعطي دلالة قابلة للإدراك**»، مفرقا في ذلك بينها وبين تعريف المحرر الإلكتروني الذي تطرقنا إليه سابقا.

بينما عرّف المشرع المغربي الكتابة الإلكترونية من خلال القانون (05-53) المشار إليه أعلاه، حيث تنص المادة (5) منه على: «**الدليل الكتابي ينتج... عن أي إشارات أو رموز أخرى ذات دلالة واضحة كيفما كانت دعامتها أو طريقة إرسالها**»، وبذلك يكون المشرع المغربي قد أقر بالكتابة الإلكترونية، والمساواة القانونية في الإثبات بين الكتابة الإلكترونية والكتابة التقليدية.

---

(1) – ذكر المشرع الجزائري مصطلح " **الكتابة المتخذة شكلا إلكترونيا**" من خلال نص المادة (323 مكرر) من القانون المدني، أين أخذ بنفس المصطلح الذي أورده المشرع الفرنسي، ويذهب بعض الفقه الفرنسي بالقول أن شكل الكتابة هو الذي تغير وليس طبيعتها، انظر في ذلك:

CAPRIOLI Eric, Le juge et la preuve électronique, Réflexion sur le projet de loi portant adaptation de la preuve aux technologies de l'information et relatif à la signature électronique, Texte présenté au colloque de Strasbourg, "Le commerce électronique : vers un nouveau droit", 8-9 octobre 1999, publié au juriscom.net (revue du droit des technologies de l'information), le 10 janvier 2000. Disponible sur : http://lthoumyre.chez.com/uni/doc/20000110.htm#fnB47.

أما عن المشرع الفرنسي، فقد نص على معنى الكتابة الإلكترونية من خلال القانون المدني، حيث تنص المادة (1316) على أن: «**معنى الكتابة يشمل كل تدوين للحروف أو العلامات والأرقام أو أي إشارة ذات دلالة تعبيرية واضحة ومفهومة، أيا كانت الدعامة التي تستخدم في إنشائها أو الوسيط الذي تنتقل عبره**» [1]، وهذا المعنى ينصرف للكتابة التقليدية والإلكترونية على حد سواء، نظرا لكونه لم يفرق بين الدعامات التي تتم عليها الكتابة.

أما في التعديل الأخير للقانون المدني الفرنسي بموجب الأمر رقم (2016-131)[2] الصادر بتاريخ (10 فيفري 2016) بشأن إصلاح قانون العقود وإثبات الالتزامات، فقد نص على الكتابة الإلكترونية بموجب المادة (1365) منه: «**الكتابة التي تتكون من سلسلة من الحروف أو الأشكال أو الأرقام أو أي إشارات أو رموز أخرى تعطي دلالة مفهومة، أيا كانت الدعامة المثبتة عليها**» [3].

باستقراء نص هذه المادة، نلاحظ أن المشرع الفرنسي في تعديله للقانون المدني لم يعرف الكتابة الإلكترونية وإنما وسع من مفهوم الكتابة العادية لتشمل أي دعامة تقليدية كانت أو إلكترونية.

كما لم يُعرف المشرع الجزائري الكتابة من قبل، إلا بعد اعتماده الكتابة الإلكترونية كوسيلة إثبات ذلك بموجب التعديل الذي مس القانون المدني سنة (2005)[4] أين نص عليها من خلال المادة (323 مكرر) من القانون المدني الجزائري: «**ينتج الإثبات بالكتابة من تسلسل حروف أو أوصاف أو أرقام أو أية علامات أو رموز ذات معنى مفهوم، مهما كانت الوسيلة التي تتضمنها، وكذا طرق إرسالها**»، يتضح من خلال نص هذه المادة أن المشرع الجزائري

---

(1)- Article (1316 Loi n° 2000-230 du 13 Mars 2000) : « **La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission** ».

)-2(Ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations. https://www.legifrance.gouv.fr/

(3)- Article (1365 loi n° 2016-131 du 10 février 2016) **: « L'écrit consiste en une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quel que soit leur support** ».

(4)- الأمر رقم 75-58 المؤرخ في 26 سبتمبر 1975 المتضمن للقانون المدني المعدل بموجب القانون رقم 10-05 المؤرخ في 20 جوان 2005، الصادر بالجريدة الرسمية بتاريخ 26 جوان 2005، العدد 44.

نص على الكتابة بنوعيها العادية والإلكترونية وذلك بقوله: "**مهما كانت الوسيلة التي تتضمنها**"، وكان من الأحسن لو استخدم مصطلح الدعامة بدل الوسيلة، لأن النص الأصلي باللغة الفرنسية جاء كالآتي **(quels que soient leur support)** والترجمة المناسبة لها أيا كانت الدعامة وليست الوسيلة.

كما أكد المشرع الجزائري أيضا على مبدأ المساواة بين الكتابة الإلكترونية والكتابة التقليدية في المادة (323 مكرر1) والتي تنص على أنه: «**يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق**».

ترتيبا على ما تقدم؛ يمكن القول أن المفهوم الحديث للكتابة صار مستقلا عن الدعامة التي تحمله. حيث عملت القوانين على تحرير مفهوم الكتابة من ارتباطه بمستوى معين من التطور التقني، سواء من حيث مادة الكتابة، طريقة تحريرها، وحتى طبيعة الدعامة المستخدمة.

2- التوقيع الإلكتروني:

لا تعتبر الكتابة دليلا كاملا في الإثبات إلا إذا كانت موقعة من صاحبها، فالتوقيع هو العنصر الثاني من عناصر المحرر، إذ أنه وفقا للقواعد العامة في الإثبات لا يعتبر أي محرر دليلا كتابيا كاملا، إلا إذا كان موقعا ممن سيحتج عليه به، أما المحررات غير الموقعة فلا يُعتد بها، إلا كمبدأ ثبوت بالكتابة، إذا ما استوفت الشروط القانونية اللازمة لاعتبارها كذلك.

وما ينطبق على المحرر التقليدي ينطبق على المحرر الإلكتروني، فلا يُعتد بالكتابة الإلكترونية في الإثبات إلا إذا كانت ممهورة بتوقيع إلكتروني يُحدد هوية صاحبها، فالتوقيع الإلكتروني هو العنصر الثاني للمحرر الإلكتروني. إلا أننا سوف نرجئ الحديث عنه بكثير من التفصيل في الفصل الثاني من هذا الباب.

ثانيا: شروط صحة المحرر الإلكتروني

على الرغم من أن الفقه والتشريعات الحديثة المتعلقة بالمعاملات الإلكترونية ساوت بين المحررات التقليدية والإلكترونية من حيث القوة الثبوتية، إلا أنها استلزمت توافر شروطا ثلاثة

في المحررات الإلكترونية حتى تكتسب هذه الحجية القانونية؛ وتتمثل هذه الشروط الثلاث في قابلية المحرر الإلكتروني للقراءة، شرط سلامة المحرر الإلكتروني، أما الشرط الثالث والأخير فهو كشف هوية الشخص الذي صدر عنه المحرر، وسنحاول شرح كل شرط بمزيد من التبسيط فيما يلي.

1- قابلية المحرر الإلكتروني للقراءة:

نجد بأن كل التشريعات التي نظّمت الاثبات بالكتابة والمحررات الإلكترونية نصت على هذا الشرط، بدءا بقانون اليونسترال النموذجي للتجارة الالكترونية لعام (1996) حيث تنص المادة (1/6) على أنه: «**عندما يشترط القانون أن تكون المعلومات مكتوبة، تستوفي رسالة البيانات ذلك إذا تيسر الاطلاع على البيانات الواردة فيها على نحو يتيح استخدامها بالرجوع إليها لاحقا**»[1].

أكدت كذلك كل التشريعات العربية والأجنبية التي تطرقنا إليها سابقا على شرط قابلية المحرر الإلكتروني للقراءة، ففي تعريفها للمحررات الإلكترونية تضمنت على مصطلحات تنص على هذا الشرط، مثل "القابلية للإدراك"، "محتوى يمكن فهمه"، "تعطي دلالة مفهومـة"، "ذات معنى مفهوم"... وغيرها مما يدل على شرط مقروئية المحرر الإلكتروني.

يقصد بشرط قراءة المحرر أن يكون مضمونه واضحا، حيث تكون الحروف أو الأرقام أو الإشارات مقروءة وقابلة للفهم، ويتحقق هذا الشرط بالنسبة للمحررات الإلكترونية بوجود برامج معلوماتية قادرة على تحويل الرموز الرياضية التي تشكل لغة الحاسوب إلى لغة مفهومة للإنسان [2].

---

(1)- يقصد بمصطلح "**إذا تيسر الاطلاع**" أن تكون المعلومات المقدمة في شكل بيانات حاسوبية مقروءة وقابلة للتفسير، كما يقصد بمصطلح" **على نحو يتيح استخدامها**" أن تشمل الاستخدام البشري وأيضا التجهيز الحاسوبي.

لمزيد من التفصيل يمكن الرجوع لدليل تشريع قانون اليونسترال النموذجي للتجارة الإلكترونية لعام (1996) الصادر بقرار الجمعية العامة رقم (162/51) في 16 ديسمبر 1996، منشورات الأمم المتحدة، نيويورك، 2000، ص 35.

(2)- **CAÏDI Stéphane,** La preuve et la conservation de l'écrit dans la société de l'information Mémoire présenté à la faculté des études supérieures en vue de l'obtention du grade de maîtrise en droit (L.L.M.), Faculté de droit, Université de Montréal, 2002, p 20.

2- شرط سلامة المحرر الإلكتروني:

يعتبر المحرر الإلكتروني سليما إذا تم إنشاءه على دعامة بصورة مستديمة ويظل على حالته التي أنشئ عليها دون أن يتعرض للتحريف أو التغيير، يقصد بشرط سلامة المحرر الإلكتروني حفظه وثباته وعدم قابليته للتعديل.

نص قانون اليونسترال النموذجي بشأن التجارة الإلكترونية على هذا الشرط من خلال المادة (10/1/أ): «**عندما يقتضي القانون الاحتفاظ بمستندات أو سجلات أو معلومات بعينها، يتحقق الوفاء بهذا المقتضى إذا تم الاحتفاظ برسائل البيانات، شريطة مراعاة الشروط التالية:**

أ- تيسر الاطلاع على المعلومات الواردة فيها على نحو يتيح استخدامها في الرجوع إليها لاحقا؛ و

ب- الاحتفاظ برسالة البيانات بالشكل الذي أُنشئت أو أُرسلت أو استُلمت به، أو بشكل يمكن إثبات أنه يمثل بدقة المعلومات التي أُنشئت أو أُرسلت أو استُلمت؛ و

ج- الاحتفاظ بالمعلومات إن وجدت، التي تمكّن من استبانة منشأ رسالة البيانات ووجهة وصولها، وتاريخ وقت إرسالها واستلامها»، كما اشترطت المادة (1/6) من القانون نفسه على أنه: «**عندما يشترط القانون أن تكون المعلومات مكتوبة، تستوفي رسالة البيانات ذلك الشرط إذا تيسر الاطلاع على البيانات الواردة فيها على نحو يتيح استخدامها بالرجوع إليها لاحقا**».

باستقراء هاتين المادتين؛ نجد أن قانون اليونسترال النموذجي قد نص على إلزامية حفظ المحررات الإلكترونية مع إمكانية الرجوع إليها لاحقا؛ ما يعني استمرارية ودوام المحررات الإلكترونية وعدم قابليتها للتحريف. وقد أصبح تحقيق هذا الشرط ممكنا بسهولة في المحررات الإلكترونية بفضل تقنيات التوقيع الإلكتروني ونظام التشفير وكذا إمكانية حفظها، حيث يكفل مقدمي خدمات الحفظ الإلكتروني[1] سلامة المحرر الإلكتروني من أي تزوير أو تحريف أو تعديل، وبهذا يتم الاعتداد بالمحرر الإلكتروني في الإثبات[2]، ويعتبر هذين النصين

---

(1) – سنتطرق بالتفصيل لنظام الحفظ الإلكتروني في الفصل الأول من الباب الثاني من هذه الأطروحة.

(2)- **باهة فاطمة**، آثار قواعد الإثبات الإلكتروني على المراكز القانونية للخصوم " دراسة مقارنة "، أطروحة مقدمة لنيل شهادة الدكتوراه في العلوم، تخصص قانون إجرائي، كلية الحقوق والعلوم السياسية، جامعة الجيلالي اليابس، سيدي بلعباس، 2017 / 2018، ص 58؛ **بلحاج بلخير**، التعاقد عبر الانترنت، دراسة مقارنة بين قانون اليونسترال والقانون الجزائري، أطروحة مقدمة

المرجعين الأساسيين لما جاءت به العديد من القوانين الحديثة في مجال الاثبات القانوني والتي سنتطرق للبعض منها تباعا فيما يلي.

نص المشرع الفرنسي من خلال المادة (1366) من القانون المدني الفرنسي على منح الكتابة الإلكترونية نفس حجية الكتابة على دعامة ورقية بشرط أن تحدد هوية مصدرها، وأن يتم إنشاؤها وحفظها في ظروف تضمن سلامتها[1]. في حين نص على حفظ المحرر الإلكتروني بموجب نص المادة (27) من القانون (575 لسنة 2004)[2] المتعلق بتعزيز الثقة في الاقتصاد الرقمي والتي أضافتها المادة (L-134-2) لقانون الاستهلاك حيث جاء نصها كالآتي: «**عندما يكون العقد مبرما بطريقة إلكترونية، وكانت قيمته تعادل أو تجاوز القيمة المحددة بموجب مرسوم يصدر بذلك، فإنه على المتعاقد المهني أن يضمن حفظ الكتابة التي تثبت العقد طوال المدة التي يحددها هذا المرسوم، وأن يضمن في أي وقت للطرف المتعاقد معه الاطلاع على المحرر متى طلب ذلك**»[3].

لنيل شهادة الدكتوراه في العلوم، تخصص قانون خاص، كلية الحقوق والعلوم السياسية، جامعة الجيلالي اليابس، سيدي بلعباس، 2020/2019، ص 303.

(1)- Article 1366 du code civil français : « **L'écrit électronique a la même force probante que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité** » Modifié par Ordonnance n°2016-131 du 10 février 2016 - art. 4.

)-2(Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, JORF n°0143 du 22 juin 2004, page 11168, texte n° 2. https://www.legifrance.gouv.fr/

(3)- Article L134-2 : « **Lorsque le contrat est conclu par voie électronique et qu'il porte sur une somme égale ou supérieure à un montant fixé par décret, le contractant professionnel assure la conservation de l'écrit qui le= =constate pendant un délai déterminé par ce même décret et en garantit à tout moment l'accès à son cocontractant si celui-ci en fait la demande ».** Créé par Loi n°2004-575 du 21 juin 2004 - art. 27 JORF 22 juin 2004.

وفي سنة 2005 صدر المرسوم الذي يحدد القيمة المذكورة أعلاه، ألا وهو المرسوم 137 لسنة 2005، والذي حددها بنحو " 120 أورو" كما حدد أيضا بالإضافة إلى قيمة المعاملة المدة القانونية الواجب الاحتفاظ بالمحرر الإلكتروني خلالها، ألا وهي (10) سنوات كاملة تبدأ من تاريخ ابرام العقد بالنسبة للعقود الفورية، أما إذا تأخر التنفيذ فتحسب المدة من تسليم المال أو تنفيذ الأداء.

Article 1 **: « Le montant visé à l'article L. 134-2 du code de la consommation est fixé à 120 Euros**. ». Article 2 : **« Le délai visé à l'article L. 134-2 du code de la consommation est fixé à dix ans à compter de la conclusion du contrat lorsque la livraison du bien ou l'exécution de la prestation est immédiate. Dans le cas contraire, le délai court à compter de la conclusion du contrat jusqu'à la date de livraison du bien ou de l'exécution de la prestation et pendant une durée de dix ans à compter de celle-ci. »** Décret n°2005-137 du 16 février 2005 pris pour l'application de l'article L. 134-2 du code de la consommation. JORF n°41 du 18 février 2005 page 2780, texte n° 27.

في حين نص المشرع الأردني على هذا الشرط بموجب قانون المعاملات الإلكترونية الأردني رقم (15 لسنة 2015) حيث أكدت المادة (8) منه على أنه: «**إذا استوجب القانون الاحتفاظ بمستند لأي سبب فيعتبر الاحتفاظ به على شكل سجل إلكتروني منتجا لآثاره على أن تتوافر فيه الشروط المنصوص عليها في المادة 7 من هذا القانون**»، وبالعودة للمادة (7/أ/1 و2) من القانون (15 لسنة 2015)، نجدها تنص على شرط إمكانية الاحتفاظ بالسجل الإلكتروني بالشكل الذي تم إنشاؤه أو إرساله أو تسلمه، وبشكل يضمن عدم إجراء أي تعديل أو تغيير فيه، وكذا حفظه على نحو يتيح الوصول إلى المعلومات الواردة فيه واستخدامها والرجوع إليها لاحقا[1].

أما عن المشرع التونسي؛ فقد نص في الفصل (4) من قانون المبادلات والتجارة الإلكترونية التونسي رقم (83 لسنة 2000) على ضمان حفظ الوثيقة الإلكترونية كما تحفظ الوثيقة الكتابية، وكذا أن تحفظ في الشكل الذي أرسلت به بالنسبة للمرسل، وفي الشكل الذي تسلمت عليه بالنسبة للمرسل إليه، مع إمكانية الاطلاع على محتواها طيلة مدة صلاحيتها[2].

في حين نص المشرع المصري من خلال المادة (18/أ) من اللائحة التنفيذية لقانون التوقيع الإلكتروني رقم (15 لسنة 2004) على أن: «... **تتحقق حجية الإثبات المقررة للكتابة الإلكترونية والمحررات الرسمية والعرفية لمنشئها، إذا توافرت الضوابط الفنية والتقنية الآتية: أ- إذا كان متاحا فنيا تحديد وقت وتاريخ إنشاء الكتابة الإلكترونية أو المحررات الإلكترونية الرسمية أو العرفية، وأن تتم هذه الإتاحة خلال نظام حفظ إلكتروني مستقل وغير خاضع لسيطرة منشئ هذه الكتابة أو تلك المحررات أو لسيطرة المعني بها**».

عند استقراء النص أعلاه، نجد أنه نص على شرطين مهمين لإضفاء الحجية على الكتابة والمحررات الإلكترونية؛ يتمثل الشرط الأول في تحديد وقت وتاريخ إنشاء الكتابة والمحرر الإلكتروني، ويعتبر هذا الشرط بالغ الأهمية لقيـــام بعض الآثـــار القانونية عليـــه، خصوصا بالنسبة لأهلية المتعاقدين. أما الشرط الثاني، وهو استقلالية نظام حفظ المحرر الإلكتروني عن

(1)- راجع المادة (7) من قانون المعاملات الإلكترونية الأردني (15 لسنة 2015)، مرجع سابق.

(2)- راجع الفصل (4) من قانون المبادلات والتجارة الإلكترونية التونسي (83 لسنة 2000)، مرجع سابق.

كل من منشئه أو من له مصلحة تتعلق به، يمنح للكتابة والمحرر الإلكتروني قوة ثبوتية لا مثيل لها، على عكس المشرع التونسي الذي جعل حفظ الوثيقة الإلكترونية تحت سيطرة كل من المرسل والمرسل إليه.

أما بالنسبة للمشرع الجزائري، فإن هذا الشرط يستفاد من خلال نص المادة (323 مكرر1) التي تقضي بأنه: «**يعتبر الاثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق بشرط إمكانية التأكد من هوية الشخص الذي أصدرها، وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها**». يتضح أن المشرع الجزائري قد صاغ هذا النص بنفس صياغة النص الفرنسي، كما أكد على أن تكون الكتابة معدة ومحفوظة في ظروف تضمن سلامتها، إلا انه لم ينص على شرط إمكانية الرجوع للكتابة وقت الحاجة والذي جاء به قانون اليونسترال النموذجي السالف ذكره؛ إلا أن حفظ الكتابة في ظروف تضمن سلامتها تُمكن لا محالة من الرجوع إليها في أي وقت[1].

3- كشف هوية مُصدر المحرر:

تنص التشريعات الحديثة على شرط ثالث لصحة المحررات الإلكترونية يتمثل في تحديد هوية مصدر المحرر الإلكتروني، وباتفاق كل الفقهاء والمشرعين لا يتحقق هذا الشرط إلا عن طريق التوقيع الإلكتروني لأنه من وظائفه الأساسية تحديد هوية الموقع[2].

نص قانون اليونسترال النموذجي للتجارة الإلكترونية على هذا الشرط من خلال المادة (2/9) منه: «**يعطى للمعلومات التي تكون على شكل رسالة بيانات ما تستحقه من حجية في**

---

(1)- **مبروك حدة**، حجية السندات الإلكترونية في الإثبات (دراسة مقارنة)، مجلة العلوم القانونية والسياسية، العدد 17، جانفي 2018، ص 43؛ **عقوني محمد، حسن عبد الرزاق**، ضوابط الاعتراف بالمحررات الالكترونية كوسيلة اثبات في العقد التجاري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 02، العدد 08، ديسمبر 2017، ص 467.

(2)- **تامر محمد سليمان الدمياطي**، إثبات التعاقد الإلكتروني عبر الانترنت دراسة مقارنة، رسالة لنيل درجة الدكتوراه في الحقوق، جامعة عين شمس، مصر، 2008، ص 617؛ **لورنس محمد عبيدات**، إثبات المحرر الإلكتروني، دار الثقافة للنشر والتوزيع، الأردن، 2009، ص 81؛ **يوسف أحمد النوافلة**، مرجع سابق، ص 80؛ **جمال عبد الرحمن محمد علي**، مرجع سابق، ص 11؛ وينظر أيضا:

CAPRIOLI Eric, Le juge et la preuve électronique, op.cit.

الإثبات، وفي تقدير حجية الرسالة يولى الاعتبار لجدارة الطريقة التي استخدمت في إنشاء أو تخزين أو إبلاغ رسالة البيانات، ولجدارة الطريقة التي استخدمت في المحافظة على سلامة المعلومات، وللطريقة التي حددت بها هوية منشئها، ولأي عامل آخر يتصل بالأمر».

كما ينص كل من المشرع التونسي [1]، الأردني [2]، الفرنسي [3]، والجزائري [4] على هذا الشرط لصحة المحررات الإلكترونية.

خلاصة ما تقدم، إذا اجتمع المحرر الإلكتروني على شرط القابلية للقراءة، سلامة المحرر، وإمكانية كشف هوية صاحبه، مع وجوب تأمينها تقنيا، حاز على حجية في الإثبات تعادل حجية المحرر التقليدي، وهو ما يطلق عليه بمبدأ التعادل الوظيفي؛ أي أن تكون المساواة كاملة بين المحررات الإلكترونية والمحررات التقليدية؛ ومتعادلة في المعاملة فيما بينها من حيث الحجية القانونية في مجال الإثبات لدرجة أن يكمل بعضها الآخر، وذلك بغرض إدماج نظام الإثبات الإلكتروني في نظام الإثبات التقليدي واعتبارها نظاما قانونيا واحدا، وكلا لا يتجزأ حتى لا تكون لأحدهما مكانة أقوى أو أضعف بين أدلة الإثبات.

---

(1)- تنص المادة (4) من قانون المبادلات والتجارة الإلكترونية التونسي رقم (83 لسنة 2000) على أن: «**يتم حفظ الوثيقة الإلكترونية على حامل إلكتروني يمكن من:**

- **الاطلاع على محتواها طيلة مدة صلاحيتها،**
- **حفظها في شكلها النهائي بصفة تضمن سلامة محتواها،**
- **حفظ المعلومات الخاصة بمصدرها ووجهتها وكذلك تاريخ ومكان ارسالها أو استلامها».**

(2)- تنص المادة (8) من قانون المعاملات الإلكترونية الأردني (15 لسنة 2015): «**إذا استوجب القانون الاحتفاظ بمستند لأي سبب فيعتبر الاحتفاظ به على شكل سجل إلكتروني منتجا لآثاره على أن تتوافر الشروط المنصوص عليها في المادة 7 من هذا القانون**»، وبالرجوع للمادة (7) نجد إمكانية التعرف على منشئ السجل الإلكتروني والمرسل إليه وتاريخ ووقت إنشائه أو إرساله أو تسلمه.

(3)- Article 1366 du code civil français : « **..., sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité** », précité.

(4)- تنص المادة (323 مكرر 1) من القانون المدني الجزائري: «**يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على ورق بشرط إمكانية التأكد من هوية الشخص الذي أصدرها ...**».

المطلب الثاني
صور المحررات الإلكترونية

تتنوع صور المحررات الإلكترونية حسب وسيلة الاتصال المستخدمة في إبرام التعاقد الالكتروني، وكذا من حيث طريقة حفظها للمحررات الإلكترونية. لذا تعتبر الدعامة التي تحفظ عليها البيانات هي وسيلة التمييز بين صور المحرر الإلكتروني، فالتطور التكنولوجي الحاصل في وسائل الاتصال والمعلومات، أدى إلى استحداث تقنيات جديدة لنقل وتخزين البيانات، حيث يتم بواسطتها التعبير عن المحرر الإلكتروني – قد تكون متصلة بشبكة الانترنت، وقد تكون غير ذلك– وعليه وجه الاختلاف الذي يميز محرر إلكتروني عن محرر إلكتروني آخر، هو الوسيلة المستخدمة في التعاقد.

بناء على ذلك، يمكن حصر صور المحررات الإلكترونية في نوعين؛ محررات إلكترونية غير مرتبطة بشبكة الإنترنت **(فرع أول)**، ومحررات إلكترونية مرتبطة بشبكة الإنترنت **(فرع ثان)**.

الفرع الأول
صور المحررات الإلكترونية غير المرتبطة بشبكة الإنترنت

يقصد بالمحررات الإلكترونية غير المرتبطة بشبكة الانترنت، تلك المحررات الناشئة عن استخدام وسيلة إلكترونية غير مرتبطة بشبكة الانترنت، وأهمها مُخرجات الهاتف **(أولا)**، مُخرجات التلكس والفاكس **(ثانيا)**، مُخرجات الحاسوب **(ثالثا)**، والدفاتر التجارية الإلكترونية **(رابعا)**، وهذا ما سنتناوله في النقاط التالية.

أولا: مُخرجات الهاتف (التسجيل الصوتي)

يُعرف الهاتف على أنه وسيلة لنقل المكالمات الشخصية بين مكانيين متصلين بخط يمر بينهما تيار كهربائي وفق ذبذبات صوت المتكلم [1]، ويعتبر وسيلة حديثة في التواصل تسمح لشخصين متواجدين في مكانيين مختلفين من التواصل مباشرة دون واسطة.

عرف الهاتف عدة تطورات حتى ظهر الهاتف النقال، والذي يعتبر أحد أشكال أدوات الاتصال اللاسلكي عن طريق شبكة من أبراج البث الموزعة على مساحة معينة، إذ تنتقل الإشارة من هاتف المرسل عبر أبراج البث المختلفة حتى تصل إلى هاتف المرسل إليه[2].

يتميز التعاقد عبر الهاتف بأنه تعاقد شفوي يتعذر إثباته ما لم يتم تسجيل المحادثات الهاتفية، ويعتبر التسجيل الصوتي من صور المحررات الإلكترونية وهو عبارة عن عملية ترجمة للتغيرات المؤقتة لموجات الصوت الخاصة بالكلام إلى نوع آخر من الموجات أو المتغّيرات الدائمة، ويحفظ التسجيل الصوتي عادة على الشريط المستخدم في جهاز التسجيل بواسطة مغناطيسية، فيتم بذلك ترجمة الصوت إلى موجات مغناطيسية تحفظ على دعامة إلكترونية وتمكن من الرجوع إليه عند الحاجة [3].

اهتم الفقه بقوة الدليل المستمد عن طريق التسجيل الصوتي ووضعه في منزلة الإقرار غير القضائي الذي يستقل قاضي الموضوع في تقديره، فيمكن أن يُعد هذا الإقرار دليلا كاملا أو مبدأ ثبوت بالكتابة يُعزز بالشهادة أو القرائن بشرط أن يتم التسجيل بعلم المُقر حتى يُنسب إليه قصد الإقرار، وفي حال إنكار الصوت يمكن للقاضي اللجوء للخبرة الفنية[4].

---

(1) – يعتبر العالم "**ألكسندر جراهم بال**" مخترع الهاتف، والهاتف كلمة تقابلها في الإنجليزية **(Téléphone)** وهي مشتقة من كلمة يونانية مركبة "**télé**" و "**phone**"، تعني الأولى الاتصال عن بعد، وتعني الثانية الصوت، فهو عبارة عن آلة لنقل الصوت بين مكانين متباعدين.

لمزيد من التفصيل حول التطورات التي لحقت بالهاتف راجع **عبد الفتاح بيومي حجازي**، مرجع سابق، ص 55.

(2)– **مراد طنجاوي**، مرجع سابق، ص 16.

(3)– **بلقاسم عبد الله**، المحررات الالكترونية وسيلة لإثبات العقد الالكتروني (دراسة مقارنة)، مذكرة لنيل شهادة الماجستير في القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013، ص31.

(4)– **عباس العبودي**، مرجع سابق، ص 280.

ثانيا: مُخرجات التلكس والفاكس

أوجدت الثورة التقنية الحديثة وسائل إلكترونية مستحدثة في التعاقد؛ كالتلكس والفاكس، أين ألغت الحضور المادي للأطراف، وقد أجازت القواعد العامة في معظم التشريعات المقارنة باستيعابها كصورة من صور التعبير عن الإرادة، وسمحت باستعمالها في إبرام التصرفات والمعاملات المدنية والتجارية وغيرها. تعتبر مُخرجات التلكس والفاكس أحد صور المحررات الإلكترونية غير المرتبطة بشبكة الإنترنت، وسنتطرق فيما يلي لكل وسيلة على حدى.

1 – مُخرجات التلكس:

لقد اعتمد في إرسال البرقيات سابقا على آلة مورس (البرق)، حيث أنه يتم إرسال البرقيات عن طريق هذه الآلة باستخدام إشارات كهربائية من جهاز المرسل إلى جهاز المرسل إليه، تمر عبر مركز سُمّي بمكتب إرسال التلغراف[1].

إلا أنه نتيجة للتطور المستمر ظهرت الحاجة للبحث عن وسيلة تربط طرفي العلاقة العقدية مباشرة ودون تدخل وسيط، فظهر التلكس الذي يتميز عن آلة مورس، أو آلة إرسال التلغراف، إذ أن التلكس لا يحتاج للمرور عبر مركز معين للإرسال.

---

(1)– كان الفرنسي "**CLAUDE Chape**» أول من صنع تلغراف سنة (1793) لكنه كان لا يسمح إلا بنقل إشارات بصرية متفق عليها مسبقا بين المرسل والمرسل إليه، وظل هذا النظام منقوصا لأنه لا يعمل ليلا أو خلال الطقس الممطر، ومع لك فقد استخدم هذا النظام بأوروبا خاصة من قبل العسكريين خلال القرن (19)، لكن التطور الهام لهذا المجال ظهر على يد "**SAMUEL Morse**" ، فقد توصل سنة (1832) إلى وضع نظام يربط بين محطتين، متى أمكن للطرف أن يبرق إشارات كهربائية، لتتلقاها المحطة الثانية بواسطة أجهزة استقبال.

لمزيد من التفصيل راجع: **علي كحلون**، الجوانب القانونية لقنوات الإتصال الحديثة والتجارة الإلكترونية، دار إسهامات في أدبيات المؤسسة، تونس، 2002، ص 28.

يعمل جهاز التلكس عن طريق تحويل الحروف المكتوبة إلى نبضات كهرومغناطيسية يتم إرسالها سلكيا أو لاسلكيا، وعند استقبال هذه النبضات تتحول إلى كلمات مطبوعة، ويتم إعداد رسائل التلكس قبل إرسالها على شريط مثقب أو شريط مغناطيسي[1].

يتسم جهاز التلكس باعتباره أحد وسائل التعاقد عن بعد بالسرعة والسرية والاتقان والوضوح[2]، إضافة للميزة الأساسية التي يتميز بها هذا الجهاز، وهي ترك أثر مادي مكتوب للرسائل التي يقوم بإرسالها، مما يسهل عبء اثبات التعاملات التي تتم عن طريقه.

أما عن الحجية القانونية للمراسلات التي تتم عن طريق جهاز التلكس، فإنه لا يوجد في نصوص الاثبات التقليدية ما يعطيها الحجية القانونية صراحة، إلا أن اعتراف المشرع الجزائري بحجية البرقيات من خلال نص المادة (329) من القانون المدني[3]، يمكنه أن يتضمن مستخرات التلكس كذلك. أما من خلال المفهوم الحديث للإثبات؛ والمتعلق خصوصا بالكتابة والتوقيع؛ فإن لمُخرجات التلكس حجية قانونية حسب الأوضاع، باعتباره محررا مكتوبا له نفس حجية المحررات المكتوبة، وهذا ما أقرته محكمة النقض الفرنسية بخصوص حجية التلكس، إذ اعتبرت أن الرسالة غير الموقعة لا تعدو إلا أن تكون مبدأ ثبوت بالكتابة وأن على من يدعي بصحتها أن يكملها بأدلة أخرى، ولكن فيما يخص النسخ الأصلية المرسلة عن طريق التلـــكس، فإنها تُعد سندا كتابيا كاملا على الرغم من عدم وجود توقيع على السند[4].

---

(1)- **إبراهيم الدسوقي أبو الليل**، الجوانب القانونية للتعاملات الإلكترونية، مجلس النشر العلمي، جامعة الكويت، 2003، ص 19.

(2)- يرجع ذلك إلى أن رسائل التلكس تعد مسبقا قبل إرسالها على شريط مثقب، أو شريط مغناطيسي، فتكون خالية من العيوب، وإذا وجدت أخطاء فيتم تصحيحها قبل إرسالها، هذا بالإضافة إلى أن الشريط الممغنط يعد بمثابة مخزن للمعلومات، فيمكن حفظها واسترجاعها وتعديلها بنفس طريقة معالجة النصوص.

لمزيد من التفاصيل راجع، **عباس العبودي**، مرجع سابق، 28.

(3)- تنص المادة (329) ق.م.ج: «**تكون للرسائل الموقع عليها قيمة الأوراق العرفية من حيث الاثبات.**

وتكون للبرقيات هذه القيمة أيضا إذا كان أصلها المودع في مكتب التصدير موقعا عليه من مرسلها، وتعتبر البرقية مطابقة لأصلها حتى يقوم الدليل على عكس ذلك.

وإذا تلف أصل البرقية فلا تعتبر نسختها إلا لمجرد الاستئناس».

(4)- **عباس العبودي**، مرجع سابق، ص 77؛ **إبراهيم الدسوقي أبو الليل**، مرجع سابق، ص 20؛ **مراد طنجاوي**، مرجع سابق، ص 19. =

2 – مُخرجات الفاكس:

يمكن تعريف جهاز الفاكس بأنه جهاز لنسخ ونقل المستندات والصور عن بعد؛ إذ يمكن بواسطته نقل الرسائل والمستندات المطبوعة أو المخطوطة بخط اليد كما هي بأصلها وبكامل محتوياتها، لذلك فهي تشمل التواقيع على عكس مستخرجات التلكس [1].

يقترن عمل هذا الجهاز بوجود الهاتف، فلا يستفيد الفرد من خدمة الفاكس إلا بوجود خط هاتفي، حيث يقوم باستنساخ صورة المحرر بواسطة أداة فاحصة تمر فوقه وتحوّله إلى نبضات كهربائية وتنقله للمرسل إليه عبر الهاتف إلى الفاكس المستقبل، أين يعيد هذا الأخير قراءة الإشارات الكهربائية وتحويلها إلى حروف أو صور، وفي الأخير طبعها لتكون مطابقة للصورة الأصل [2].

أما عن حجية مُخرجات الفاكس، فقد حظيت بالقبول القانوني إذ أشار إليها القانون النموذجي بشأن التجارة الإلكترونية لسنة (1996) من خلال المادة (1/2) منه، أما عن المشرع الجزائري فيمكن القول أنه اعترف بها بشكل عام من خلال المادة (329) من القانون المدني سالفة الذكر، حيث منح المحررات الناشئة عن الفاكس والمعبر عنها بالبرقية ذات القيمة الممنوحة للمحررات العرفية.

ثالثا: مُخرجات الحاسوب

يعتبر جهاز الحاسوب[3]، من أهم الأجهزة العلمية المتطورة، إذ يرتكز عمله على مراحل ثلاث: مرحلة إدخال البيانات، ثم مرحلة معالجتها، وفي الأخير مرحلة إخراجها إلى العالم

= تجب الإشارة إلى أن من بين عيوب جهاز التلكس، أنه لا يرسل الرسوم التوضيحية والتواقيع وغيرها من الهوامش، أي أن مستخرجات التلكس هي محررات بدون توقيع. مشار إليه لدى: **يوسف أحمد النوافلة**، مرجع سابق، ص 272.

(1)– **بلقاسم عبد الله**، مرجع سابق، ص 34.

(2)– **العياشي زرزار**، تكنولوجيا المعلومات والاتصالات وأثرها على النشاط الاقتصادي وظهور الاقتصاد الرقمي، مجلة البحوث والدراسات الإنسانية، جامعة 20 أوت 1955، سكيكدة، العدد06، نوفمبر 2010، ص 218.

(3)– الحاسوب بالإنجليزية (**Computer**) مشتق من الفعل (**Compte**) أي عدد من الحساب، وفي ترجمته أطلق عليه اسم "الكمبيوتر"، "الحاسب الآلي"، "العقل الإلكتروني"... وغيرها. إلا أن المنظمة العربية للمواصفات والمقاييس أطلقت عليه اسم=

الخارجي على شكل قابل للقراءة؛ منها ما يأخذ شكلا ورقيا، وهناك مخرجات تأخذ شكلا إلكترونيا[1]، فالمخرجات الورقية تكون عن طريق الطابعات، أما المخرجات في الشكل الإلكتروني فتسجل على حامل إلكتروني مثل القرص المرن أو القرص الممغنط، وسنوضح ذلك تباعا.

1- المخرجات الورقية:

تتمثل في المُخرجات المسجلة على دعامات مادية، وهذه الأخيرة هي التي تُشكل دليلا في الإثبات وتحمل بين طياتها كتابة على دعامة مادية واضحة وملموسة ويمكن الاحتفاظ بها والرجوع إليها عند الحاجة، إذ أن المعلومات والبيانات المحررة والمعالجة على جهاز الحاسوب تُخرج على شكل ورقي بواسطة الطابعات المتصلة بالحاسوب [2].

تعتبر مُخرجات الكمبيوتر الورقية دليلا كتابيا، إذ يمكن القول بإنها تجسيد كامل لفكرة المحرر الإلكتروني، وحتى تعتبر دليلا في الإثبات، وجب احتوائها على عناصر المحرر الإلكتروني من كتابة وتوقيع إلكترونيين.

2- المُخرجات الإلكترونية:

يوجد نوع ثان من مُخرجات الحاسوب يُخزن على دعامات غير ورقية، يُطلق عليها مصطلح المُخرجات الإلكترونية، تستخدم لإدخال وإخراج البيانات والمعلومات من الحاسوب وتخزين المعلومات فيه، وهي أجهزة مساعدة لذاكرة الحاسوب الرئيسية الموجودة داخله، كما أنها

="الحاسوب"، كما صدر معجم الحاسبات عن مجمع اللغة العربية سنة (1987) دون إضافة كلمة إلكترونية أو آلية إلى كلمة الحاسبات. وهو يتكون من وحدات إدخال ووحدات إخراج، يستعمل لمعالجة المعلومات وتحرير النصوص والمستندات وحفظها وتخزينها وطباعتها.

راجع في ذلك: **فيصل سعيد الغريب**، التوقيع الإلكتروني وحجيته في الإثبات، المنظمة العربية للتنمية الإدارية، مصر، 2005، ص 145.

(1)- عاطف عبد الحميد حسن، مبدأ الثبوت بالكتابة في ضوء التطور التكنولوجي الحديث، دار النهضة العربية، مصر، 2002، ص 73.

(2)- يوسف أحمد النوافلة، الإثبات الإلكتروني في المواد المدنية والمصرفية -دراسة مقارنة-، دار الثقافة للنشر والتوزيع، الأردن 2012، ص 45.

تختلف عن المخرجات الورقية إذ أنها مصنوعة من مواد بلاستيكية أو معدنية وأهمها المصغرات الفيلمية والأقراص الممغنطة.

أ- المصغرات الفيلمية:

تقوم المصغرات الفيلمية بأشكالها المختلفة على فكرة إدخال المحرر أو الورقة الأصلية إلى أجهزة تستنسخ عنها صورة وتخزنها بشكل مصغر، أو مضغوط، يتيح استرجاعها وإعادة طباعة نسخة عنها، وتقنيا فإن المُخزن في الذاكرة الإلكترونية هو صورة عن الأصل والمُستخرج من الجهاز التقني صورة عن الأصل أيضا [1].

تمتاز هذه المصغرات الفيلمية بالقدرة الهائلة على حفظ المعلومات ولمدة طويلة، فضلا عن إمكانية الحصول على نسخ منها في أي وقت، إضافة إلى سهولة نقلها وتداولها، مما أدى إلى تقليص النفقات وحل مشكل تراكم وثائق الأرشيف [2].

ب- الأقراص الممغنطة:

تعتبر أحد أكثر وسائل تخزين المحررات الإلكترونية استخداما، وهي عبارة عن أسطوانة مغطاة بمادة ممغنطة صلبة، يتم تخزين البيانات عليها في شكل حروف أو رموز متتابعة، عبر مسارات متسلسلة تتحد معها مركزيا. تتميز بالسرعة في الحفظ والكثافة العالية في التخزين، ومن أهم أنواعها القرص الصلب [3]، والقرص المرن[4].

---

(1)- الغريب فيصل سعيد، مرجع سابق، ص 155.

(2)- عائشة قصار الليل، حجية المحرر والتوقيع الالكتروني في الإثبات – دراسة تحليلية مقارنة – رسالة مقدمة لنيل شهادة الدكتوراه علوم في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، 2016-2017، ص 33.

(3)- القرص الصلب: عبارة عن قرص معدني رقيق مغطى بمادة مغناطيسية يتم صباغته بواسطة سبائك الألمنيوم، غير قابل للتداول ولا يتم تحريكه إلا بفصل وصلاته من الوحدة المركزية، يتم من خلاله تخزين أنظمة التشغيل والبرامج التطبيقية ولغات البرمجة والملفات المستخدمة، يتميز بالقدرة العالية على التخزين إضافة للسرعة في التسجيل واسترجاع البيانات. راجع **لورنس محمد عبيدات**، مرجع سابق، ص 85؛ **يوسف أحمد النوافلة**، الاثبات الإلكتروني في المواد المدنية والمصرفية، مرجع سابق، ص51.

(4)- القرص المرن: عبارة عن قرص دائري به فتحة كبيرة نسبيا لحجم القرص والتي تتصل من خلالها بوحدة إدارة الأقراص، مصنوع من أداة رقيقة جدا من البلاستيك مغطاة بطبقة من مادة ممغنطة حساسة من أكسيد الحديد، تخزن فيه البيانات والبرامج، ويتم تعديلها ومحوها عند الاقتضاء. راجع: **عائشة قصار الليل**، المرجع نفسه، ص 35.

أما عن حجية هذه المخرجات الإلكترونية السالف ذكرها، نجد أن المشرع الجزائري لم يتطرق لها بالتنظيم، إلا أنه وبالعودة للقواعد العامة في الاثبات المنصوص عليها في القانون المدني نجد أن المادة (323 مكرر) منه تنص على أنه: «**ينتج الاثبات بالكتابة من تسلسل حروف أو أوصاف أو أرقام أو أية علامات أو رموز ذات معنى مفهوم، مهما كانت الوسيلة التي تتضمنها، وكذا طرق إرسالها**». ومن خلال تعريف المحرر الإلكتروني الذي توصلنا إليه سابقا بأنه عبارة عن بيانات مكتوبة في شكل إلكتروني قابلة للإدراك، تنشأ أو تخزن أو ترسل أو تستلم باستخدام نظام المعالجة الآلية للمعطيات، تعبر عن إرادة صاحبها، ومحفوظة ضمن ظروف تضمن سلامتها للرجوع إليها عند الحاجة، وهو ما نجده ينطبق على تعريف المُخرجات الإلكترونية للحاسوب مما يفتح المجال للاعتراف بحجيتها في الاثبات.

رابعا: الدفاتر التجارية الإلكترونية

ألزمت أغلب التشريعات ومنها المشرع الجزائري [1]، التاجر بمسك دفاتر تجارية يقيد فيها جميع العمليات التجارية التي يقوم بها خلال مزاولته لنشاطه التجاري، إذ تعتبر هذه الدفاتر العمود الرئيس في تثبيت مصاريفه اليومية. وتوثيق قيوده المحاسبية. ونظرا لأهمية مسك هذه الدفاتر التجارية باعتبارها أهم الالتزامات المهنية الواقعة على عاتق التجار، فقد تم النص عليها في معظم التشريعات التجارية [2].

غير أن ظهور التجارة الإلكترونية، وتضخّم عدد العمليات التجارية الناتج عن استخدام مختلف تقنيات الوسائط الإلكترونية، أدى إلى ظهور نوع جديد من الدفاتر تتماشى والتطور التقني الحاصل، أطلق عليها مصطلح "الدفاتر التجارية الإلكترونية".

---

(1)- راجع المواد (9-10) من الأمر رقم 75- 59 مؤرخ في 29 جوان 1975، يتضمن التقنين التجاري، معدل ومتمم بموجب القانون رقم 05 -02، مؤرخ في 06 فيفري 2005، ج ر ع 11 صادر بتاريخ 09 فيفري 2005.

(2)- المواد (21-29) من قانون التجارة المصري رقم 17 لعام 1999 المنشور ج ر ع 19، المواد (19 -26) من مدونة التجارة المغربية المنشورة ج ر ع 4418 الصادرة بتاريخ 03 أكتوبر 1996، المادة (16) من قانون التجارة والأنظمة الأردني رقم 12 لسنة 1966 المشور ج ر ع 1910 بتاريخ 30-03-1966.

عرفّ بعض الفقه الدفاتر التجارية الإلكترونية على أنها: «**عبارة عن استخدام وسيلة القيد الإلكتروني في تدوين وحفظ المعاملات التجارية للتاجر، أو هي سجلات إلكترونية يدون فيها التاجر كافة مدخلات ومخرجات معاملاته التجارية ليتحدد على ضوئها مركزه المالي**»[1]، في حين عرفها جانب ثان من الفقه بأنها: «**قيد التاجر لعملياته التجارية بالوجه الذي يتطلبه القانون لبيان مركزه المالي بوسيلة إلكترونية مثل الحاسب الآلي وغيره من الأجهزة التقنية الحديثة بطريقة منتظمة تمنع أي تعديلات أو محو لبياناتها**»[2].

وعليه يمكن تعريف الدفاتر التجارية الإلكترونية على أنها قيد إلكتروني لعمليات التاجر التجارية تبين من خلالها مركزه المالي.

بالرجوع للقانون التجاري الجزائري، نجد أن المشرع الجزائري لم يقم بتنظيم هذا النوع المستجد من الدفاتر التجارية، وإنما اعترف به ضمنيا من خلال القانون (07-11) المتضمـــن النظام المحاسبي المالي [3]، أين أطلق عليه مصطلح المحاسبة المالية بدل الدفـــاتر التجارية، من خلال المادة (4) منه، والتي ألزمت كل من الشركات الخاضعة لأحكام القانون التجاري، التعاونيات، الأشخاص الطبيعيين أو المعنويين المنتجين للسلع أو الخدمات التجارية وغير التجارية إذا كانوا يمارسون نشاطات اقتصادية مبنية على عمليات متكررة، وكل الأشخاص الطبيعيين أو المعنويين الخاضعين لذلك بموجب نص قانوني أو تنظيمي بمسك محاسبة مالية.

---

(1)- أحمد محمود المساعدة، حجية الدفاتر التجارية الإلكترونية في الإثبات، مجلة العلوم القانونية والسياسية، جامعة الوادي، العدد 04، جانفي 2012، ص 105.

(2)- مجيد أحمد إبراهيم، الدفاتر التجارية الإلكترونية وحجيتها في الإثبات، المجلة الأكاديمية للبحث القانوني، العراق، المجلد 17، العدد01، سنة 2018، ص 71.

(3)- القانون رقم (07-11) المؤرخ في 15 ذي القعدة 1428 الموافق 25 نوفمبر 2007 المتضمن النظام المحاسبي المالي، ج ر ع 74 صادر في 25-11-2007.

إلا أنه وبصدور المرسوم التنفيذي رقم (19-89)[1]، المحدد لكيفيات حفظ سجلات المعاملات التجارية الإلكترونية وإرسالها إلى المركز الوطني للسجل التجاري، وضع المشرع الجزائري من خلال المادة (2) منه تعريفا صريحا لسجلات المعاملات التجارية، إذ نص على أنها: «**ملف إلكتروني يخزن فيه المورد عناصر المعاملات التجارية والمتمثلة في العقد والفاتورة ووصولات الاستلام**».

الفرع الثاني
صور المحررات الإلكترونية المرتبطة بشبكة الانترنت

إضافة لصور المحرر الإلكتروني غير المرتبطة بشبكة الإنترنت والتي أوضحنا معناها في النقطة السابقة، هناك صور أخرى مرتبطة بشبكة الإنترنت تتمثل أساسا في البريد الإلكتروني (**أولا**)، ورسائل الإنترنت(**ثانيا**).

أولا: البريد الإلكتروني

يعد البريد الإلكتروني[2]، أحد أهم الوسائل المستحدثة في تكنولوجيا الاتصالات، إذ أنه من أهم تطبيقات الإنترنت وأكثرها استخداما، وقد فرض نفسه إلى جانب الوسائل التقليدية للاتصال بفضل سرعته الفائقة وتكلفته البسيطة وسهولة استخدامه ومرونته.

---

(1)- مرسوم تنفيذي رقم (**19-89**) المؤرخ في **5** مارس **2019**، المحدد لكيفيات حفظ سجلات المعاملات التجارية الالكترونية وإرسالها إلى المركز الوطني للسجل التجاري، ج ر ع 17، صادر في 17 مارس 2019.

(**2**)- ظهر البريد الإلكتروني في أمريكا على يد العالم الأمريكي "**راي توملينسون**" "**RAY TOMLINSON**" ، حيث كان يعمل في شركة "**BBN**" والتي كُلفت من قبل وزارة الدفاع ببناء شبكة تربط المعاهد العلمية والجامعات بعضها ببعض أين ظهرت "الأربانات" "**ARPANET**"، شارك "**راي توملينسون**" في هذا المشروع باختراعه برنامج لكتابة الرسائل على شبكة الإنترنت لتمكين مستخدمي شبكة الأربانات من تبادل الرسائل وسمي هذا المشروع ب "**SEND MESSAGE**"، حيث يمكن هذا البرنامج من صنع ملف على الحاسوب الذي يتداول عليه شخصين أو أكثر، توضع فيه الرسالة ليتمكن الموظف الذي يأتي لاحقا من قراءتها؛ حيث لم يكن صندوق البريد في البداية سوى ملف يكتب فيه المستخدم رسالته، ولا يمكن للقارئ إعادة الكتابة عليه أو تعديله، وإنما يسمح له بقراءته فقط. ثم اخترع فيما بعد برنامجا آخر مكنه من نقل الملفات من حاسوب لحاسوب آخر سماه ب "**CYPENT**" ، ليقوم فيما بعد بدمج البرنامجين معا مما أدى لظهور البريد الإلكتروني، إلا أنه واجهته مشكلة عدم قدرة تحديد مكان إرسال الرسالة فابتكر رمز خاص سنة (1971) لا يستخدم في الأسماء، ليفصل به بين اسم=

عرف جانب من الفقه البريد الإلكتروني بأنه: «**مكنة التبادل الإلكتروني غير المتزامن للرسائل بين أجهزة الحاسب الآلي**»[1]. بينما عرّفه البعض بأنه: «**طريقة تسمح بتبادل الرسائل المكتوبة بين الأجهزة المتصلة بشبكة المعلومات**»[2]. في حين نجد أن البعض الآخر قد عرفه بأنه: «**تلك المستندات التي يتم إرسالها أو استلامها بواسطة نظام اتصالات بريدي إلكتروني وتتضمن ملحوظات مختصرة ذات طابع شكلي حقيقي، ويمكنه استصحاب مرفقات به مثل معالجة الكلمات وأية مستندات أخرى يتم إرسالها رفقة الرسالة ذاتها**»[3]. وقد عرفته اللجنة العامة للتحديثات اللغوية والمصطلحات في فرنسا[4] بأنه: «**وثيقة معلوماتية يحررها أو يرسلها أو يطلع عليها المستخدم عن طريق الاتصال بشبكة معلومات**»[5].

كما تطرقت بعض التشريعات لتعريف مصطلح البريد الإلكتروني، فنجد مثلا أن المشرع الفرنسي تناوله من خلال قانون الثقة في الاقتصاد الرقمي رقم (575/2004) الصادر في (22 جوان 2004) أين تنص على أنه: «**كل رسالة سواء كانت نصية أو صوتية أو مرفق بها صور أو أصوات، ويتم ارسالها عبر شبكة اتصالات عامة، وتخزن عند أحد خوادم تلك الشبكة أو في المعدات الطرفية للمرسل إليه ليتمكن هذا الأخير من استعادتها**»[6].

بينما عرّف المشرع الجزائري البريد الإلكتروني من خلال المادة (2) من المرسوم التنفيذي رقم (98-257) الذي يضبط شروط وكيفيات إقامة خدمات الانترنت واستغلالها[7] على أنه:

=الشخص والموقع الإلكتروني، وكان ذلك الرمز (@)، ليضع أول عنوان بريد إلكتروني في تاريخ الانترنت وهو (**Tomlinson@bbn-tenexa**).

نقلا عن **خالد ممدوح إبراهيم**، حجية البريد الإلكتروني في الاثبات، دار الفكر الجامعي، مصر، 2010، ص 38.

(**1**)- **مصطفى عثمان عبد الله**، حجية البريد الإلكتروني في إثبات المعاملات المدنية والتجارية، مجلة كلية الشريعة والقانون، جامعة الامام المهدي، العدد الأول، السنة الأولى، يناير 2017، ص 227.

(**2**)- **خالد حسن أحمد لطفي**، المستند الإلكتروني ووسائل اثباته وحمايته، دار الفكر الجامعي، مصر، 2018، ص 309.

(**3**)- **خالد ممدوح إبراهيم**، مرجع سابق، ص 42.

)-4(Commission générale de terminologie et de néologie.

)-5(Courrier électronique: Document informatisé qu'un utilisateur saisit, envoie ou consultent différé par l'intermédiaire d'un réseau". J.O n° 141 du 20 juin 2003, p.10403.

(**6**)- **رمضان قنفود**، الطبيعة القانونية للبريد الالكتروني ومدى حجيته في الاثبات، مجلة الدراسات القانونية، جامعة يحيى فارس، المدية، العدد الثاني، المجلد الثاني، ص 163؛ **سليماني مصطفى**، مرجع سابق، ص 116.

(**7**)- مرسوم تنفيذي رقم (92-257) مؤرخ في 25 غشت 1998، الذي يضبط شروط وكيفيات إقامة خدمات انترنت واستغلالها، ج.ر.ع 63، صادر في 26 غشت 1998.

«**خدمات تبادل رسائل إلكترونية بين المستخدمين**»، ويعتبر هذا التعريف مقتضبا وناقصا جدا، ليُعرف فيما بعد رسالة البيانات والتي تعتبر من مُخرجات البريد الإلكتروني من خلال المرسوم التنفيذي (01-123) المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية، وعلى مختلف خدمات المواصلات السلكية واللاسلكية[1]، بأنها: «**تبادل وقراءة وتخزين معلومات في شكل رسائل معطيات بين الموزعات الموجودة في مواقع متباعدة، ويمكن المرسل إليه (أو المرسل إليهم) قراءة الرسالة المبعوثة في وقت حقيقي، أو في وقت مؤجل**».

من خلال التعريفات التي تطرقنا إليها أعلاه، نلاحظ وجود اختلاف في تعريف البريد الإلكتروني. فالمشرع الفرنسي يرى بأنه عبارة عن رسالة نصية كانت أو صوتية أو مرئية، في حين يرى المشرع الجزائري بأنه عبارة عن نظام إرسال، وهناك فرق بين نظام الإرسال الذي يُعد وسيلة لإرسال الرسالة والتي تعتبر مجموعة حروف أو رموز أو أرقام ...الخ.

يمكن تصنيف رسائل البريد الإلكتروني لثلاثة أنواع، رسائل عادية غير موقعة إلكترونيا، رسائل موقعة إلكترونيا، ورسائل موصى عليها، وسنوضح ذلك فيما يلي:

1 - رسائل البريد الإلكتروني غير الموقعة:

تعتبر رسائل البريد الإلكتروني غير الموقعة الأكثر شيوعا عبر شبكة الانترنت، إلا أنه لا قيمة لها في الاثبات لعدم احتوائها على توقيع[2]، إذ لا يمكن التحقق من هوية المرسل أو مصداقية محتواها نظرا لعدم وجود توقيع إلكتروني يحدد هوية الموقع.

---

(1)- المرسوم التنفيذي رقم (01-123) مؤرخ في 09 ماي 2001، المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية، وعلى مختلف خدمات المواصلات السلكية واللاسلكية، والملحق المكمل له، ج.ر.ع 27، صادر في 13 ماي 2001.

(2)- **يوسف أحمد النوافلة**، الاثبات الإلكتروني في المواد المدنية والمصرفية، المرجع السابق، ص 143.

2- رسائل البريد الإلكتروني الموقعة إلكترونيا:

تكون رسائل البريد الإلكتروني في هذه الحالة موقعة إلكترونيا من قبل صاحبها، إما عن طريق كتابة الاسم واللقب كاملين أو الأحرف الأولى منهما بواسطة لوحة المفاتيح في آخر الرسالة، أو عن طريق مسح التوقيع التقليدي للمرسل بواسطة الماسح الضوئي ثم إدخالها وحفظها في جهاز الحاسوب ليتم إضافتها فيما بعد لرسالة البريد الإلكتروني، لكن هل تصلح الصور السابقة للاعتداد بهما كتوقيع إلكتروني؟

تنعدم في كلا الصورتين السابقتين تحقق وظيفة التوقيع الإلكتروني؛ ألا وهي تحديد هوية الموقع[1]، فكتابة الاسم في نهاية البريد الإلكتروني لا تصلح أن تكون وسيلة لتحديد أن شخص معين هو الذي قام بتحرير مضمون البريد الإلكتروني وأنه ارتضى بما ورد به، فيمكن لأي شخص أن ينشأ حساب بريدي إلكتروني وكتابة المعلومات التي يريدها عليه. والأمر ذاته بالنسبة للتوقيع باستعمال الماسح الضوئي، إذ تعتبر هذه الطريقة غير آمنة وغير موثوقة لإمكانية الحصول على صورة التوقيع لأي شخص، وإعادة استخدامها في محرر لا علاقة له به.

3- رسائل البريد الإلكتروني الموصى عليها:

عرّفت المادة (9/2) من التوجيه الأوروبي رقم (15 لسنة 1997) بشأن السوق الداخلي للخدمات البريدية "البريد الموصى" بأنه: «**خدمة تتم وفق إجراءات تكفل ضمان الإرسال ضد مخاطر الفقد أو السرقة أو التلف وتوفى للمرسل لقاء مبلغ جزافي يدفعه كدليل على إيداع الرسالة لدى هيئة البريد وكذلك عند الضرورة وبناء على طلبه لإثبات استلام المرسل إليه الرسالة**» [2].

(1)- **محمد محمد سادات**، أثر تنوع التوقيعات الالكترونية على حجية العقود العرفية الالكترونية، مجلة صوت القانون، العدد السابع، الجزء الثاني، 2017، ص 152؛ **مصطفى عثمان عبد الله**، مرجع سابق، ص 230؛ **يوسف أحمد النوافلة**، الاثبات الإلكتروني في المواد المدنية والمصرفية، مرجع سابق، ص 143.

(2)- **خالد حسن أحمد لطفي**، مرجع سابق، ص 315؛ **يوسف أحمد النوافلة**، الإثبات الإلكتروني في المواد المدنية والمصرفية، مرجع سابق، ص 144.

تقوم خدمة البريد الموصى عليه على توفر علاقة بين ثلاثة أطراف؛ المرسل والمرسل إليه ومقدم الخدمة، إذ يجب على المرسل إثبات هويته لدى مقدم الخدمة وهو هيئة البريد الذي يلعب دور جهة التصديق. ليرسل هذا الأخير وصل إلى المرسل إليه يثبت من خلاله هوية المرسل ووجود رسالة إلكترونية يمكن تحميلها من الموقع الإلكتروني لمزود الخدمة، وعند تحميل الرسالة يرسل مقدم الخدمة إلى المرسل وصلا يبين فيه تاريخ وساعة استلام المرسل إليه الرسالة [1].

يمتاز هذا البريد بنوع من الحماية نظرا لتدخل طرف ثالث لإثبات هوية المرسل، ونظرا لما يقدمه هذا النوع من البريد من مزايا خصوصا في مجال الإثبات اهتمت التشريعات بتنظيمه وإضفاء الحجية عليه، وهو ما سنوضحه لاحقا.

ثانيا: رسائل الانترنت

أتاحت شبكة الانترنت للمستخدمين العديد من مواقع الدردشة وتبادل الرسائل الخطية والصوتية والمرئية، مثل رسائل برامج المحادثات، حيث تتيح هذه البرامج للمستخدمين الاتصال بالصوت والصورة عن طريق جهازي الكاميرا والميكروفون المثبتين على الحاسوب، مع توفير خاصية التواصل عن طريق الكتابة في الوقت نفسه[2]، إضافة لهذه المواقع، ظهرت مواقع أخرى تعنى بالتعارف والتواصل بين الأشخاص، عُرفت بمواقع التواصل الاجتماعي[3] مثل "الفيسبوك" **"Facebook"**، "التويتر" **"Tweeter"**، "الواتس آب"

---

(1)- **زينب غريب**، حجية البريد الإلكتروني في الاثبات، مجلة العلوم القانونية (مجلة إلكترونية)، مقال منشور على الموقع: https://www.marocdroit.com .

(2)- **حسن عبد الباسط جميعي**، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الإنترنت، دار النهضة العربية، مصر، 2000، ص 8.

(3)- كان أول ظهور لهذه الشبكات في منتصف التسعينات من القرن الماضي، والسبب في وصف هذه الشبكات بالاجتماعية أنها تتيح التواصل بشكل مباشر مع مشاهير السياسة والآداب والفنون والرياضة ومع الأقارب والأصدقاء القدماء والجدد ومع زملاء الدراسة أو العمل، ومن ثم تقوي الروابط بين أعضاء هذه الشبكات في فضاء الإنترنت وتتيح لهم تبادل الرأي ووجهات النظر حول موضوعات شتى، ويُعد موقع "فيسبوك" الأوسع انتشارا على مستوى العالم؛ إذ يتجاوز عدد مستخدميه المليار شخص. =

"**Whatsapp**"، و"لينكد إن" "**LinkedIn**"، إذ تمكن المستخدمين من التواصل عن طريق الكتابة والاتصال بالصوت والصورة أيضا.

يصعب وضع تعريف جامع لكل صور مواقع التواصل الاجتماعي لتعدد صورها، إلا أنه يمكن تعريفها بوجه عام على أنها: «**الخدمات عبر الإنترنت التي تهدف إلى إنشاء وربط مجموعات من الأشخاص يتشاركون أنشطة أو مصالح مشتركة بينهم، أو لديهم الرغبة في التعرف على ميول وأنشطة أشخاص آخرين، وتتيح لهم العديد من الميزات التي تساعدهم على التفاعل فيما بينهم**» [(1)].

وعليه تمكّن وسائل التواصل الاجتماعي المستخدمين من التواصل عن طريق الكتابة والاتصال بالصوت والصورة أيضا، وكل هذه الطرق تعتبر من صور المحررات الإلكترونية، غير أنه يثور التساؤل حول مدى الاعتداد بهذه المحررات في الإثبات؟

لا يوجد من الناحية الفعلية ما يحول دون قيام المستخدم لشبكات التواصل الاجتماعي من إدراج بياناته الشخصية بشكل غير دقيق أو مخالف للواقع، كأن يدرج اسما مغايرا لاسمه، أو يحدد تاريخ ميلاد وهمي يختلف عن تاريخ ميلاده الفعلي؛ مما يعيق تحديد هوية المستخدم الفعلي؛ مما ينتج عنه انعدام قيمتها في الإثبات.

نخلص مما سبق، إلى أن المحررات الإلكترونية ما هي إلا امتداد للمحررات التقليدية، وأن اختلاف الدعامة التي تقوم عليها لا تؤدي إلى إنقاص قيمتها في الإثبات إذا ما استوفت الشروط القانونية لقيامها، من تحديد هوية الشخص المنسوب إليه المحرر الإلكتروني، وكذا سلامة هذا الأخير من مخاطر التعديل والتحريف. وهو ما جعل العديد من الدول تصدر قوانين خاصة تُعنى بهذا النوع المستحدث من الأدلة الكتابية، أو القيام بتعديل القواعد

= لمزيد من التفصيل أنظر: **علي السيد حسين أبو دياب**، أضواء على حجية الرسائل في الإثبات في مواقع التواصل الاجتماعي، مجلة كلية الشريعة والقانون، العدد 32، الجزء3، مصر، يونيو 2017، ص 958.

https://mksq.journals.ekb.eg ›

(1)- **علي السيد حسين أبو دياب**، المرجع نفسه، ص 958

القانونية العامة لتشمله وتُقر بحجيته في الإثبات وهو جوهر ما سنتطرق إليه في المبحث الثاني، إذ سنين من خلاله الحجية القانونية المقررة لهذه المحررات الإلكترونية في الإثبات.

المبحث الثاني
حجية المحررات الإلكترونية في الإثبات

أقرّت التشريعات الدولية والوطنية المتعلقة بالإثبات في المعاملات الإلكترونية بمبدأ التعادل الوظيفي بين المحررات التقليدية والمحررات الإلكترونية، والمساواة فيما بينهما من ناحية الحجية القانونية في الإثبات، وعدم التنكر لقيمة المحررات الإلكترونية في الإثبات لمجرد أنها تقوم على وسيط افتراضي غير محسوس.

إن الاعتراف بمبدأ التعادل الوظيفي بين المحررات التقليدية والمحـــــررات الإلكترونية، يترتب عليه إقرارا بالمساواة بين المحررات الرسمية التقليدية والمحررات الرسمية الإلكترونية من حيث الحجية القانونية في الإثبات، والأمر ذاته بالنسبة للمساواة بين المحررات العرفية التقليدية والمحررات العرفية الإلكترونية.

إن المحررات الرسمية هي المحررات التي يقوم بتحريرها موظف عام مختص أو ضابط عمومي أو شخص مكلف بخدمة عامة، وتكون دائمـــــــا موقعة ممن صدرت منهم، وتعتبر دليلا كتابيا كاملا. أما المحررات العرفية فهي التي تصدر من الأفراد فيما بينهم، وتنقسم إلى نوعين؛ محررات عرفية معدة للإثبات، ومحررات عرفية غير معدة للإثبات.

ولما كانت القواعد العامة في الإثبات تميّز بين مدى الحجية المقررة للمحررات الرسمية التقليدية والمحررات العرفية التقليدية في الإثبات بناء على شروط قيامها، الأمر الذي يقضي بالتمييز بين المحررات الرسمية الإلكترونية والمحررات العرفية الإلكترونية كذلك.

غير أن اختلاف كل من الدعامة التي تقوم عليها المحررات التقليدية والإلكترونية يدفعنا للتساؤل حول ما إذا كانت شروط حجية نوعي المحررات التقليدية –الرسمية والعرفية– هي ذاتها المقررة بالنسبة للمحررات الإلكترونية –الرسمية والعرفية–، أم أنه لا يمكن الاكتفاء بتطبيق القواعد العامة المخصصة للإثبات التقليدي على الإثبات الإلكتروني، بل يستلزم الأمر إصدار تنظيم قانوني مستقل يتسم بالدقة ويحيط بجميع جوانبها التقنية.

لإزالة الغموض عن كل ما سبق ذكره سنتطرق من خلال هذا المبحث لكل من القيمة الثبوتية للمحررات الرسمية الإلكترونية **(مطلب أول)**، ثم للقيمة الثبوتية للمحررات العرفية الإلكترونية **(مطلب ثان)**.

المطلب الأول

القيمة الثبوتية للمحررات الرسمية الإلكترونية

يُعتبر المحرر الرسمي المثبت للتصرف القانوني أقوى المحررات؛ سواء من حيث الإجراءات المُعقدة لتحريره أو من حيث حجيته في الإثبات؛ إذ لا يزال محط أنظار المتعاملين لما يضفيه من ثقة وأمن على التصرفات القانونية. وفي ظل المستجدات التي أحدثتها الثورة المعلوماتية في مجال إبرام التصرفات القانونية ظهرت إلى الساحة القانونية المحررات الرسمية الإلكترونية، الأمر الذي دعى المشرعين على مختلف المستويات لمحاولة تنظيمها بما يتلاءم مع البيئة التقنية القائمة عليها حفاظا على بنيتها القانونية من جهة، وكذا توفير الحماية اللازمة لها من جهة أخرى.

على الرغم من اعتراف المشرع الجزائري بالكتابة الإلكترونية ومساواتها بالكتابة التقليدية، إلا أننا نجده من خلال المادة (3) من القانون (18-05) المتعلق بالتجارة الإلكترونية قد منع كل معاملة بسلعة أو خدمة تستوجب إعداد عقد رسمي، على الرغم مما تكتسيه هذه المحررات من أهمية بالغة في مجال المعاملات.

وفي ظل غياب تنظيم تشريعي جزائري للمحررات الرسمية الإلكترونية، سنحاول التطرق بالدراسة للمستجدات التي جاءت بها القوانين المقارنة في تنظيمها للمحررات الرسمية الإلكترونية والبحث في إمكانية تطبيقها على مستوى النظام القانوني الجزائري، بدءا بالبحث في شروط صحة المحرر الرسمي الإلكتروني **(فرع أول)**، عناصر حجيته **(فرع ثان)**، وكذا حجية صور المحرر الرسمي الإلكتروني **(فرع ثالث)**، كل هذا وفقا للقواعد العامة المقررة لشروط حجية المحررات الرسمية، والقواعد الخاصة المستحدثة التي عنيت بتنظيمها.

الفرع الأول
شروط صحة المحرر الرسمي الإلكتروني

عُرّف المحرر الرسمي الإلكتروني بأنه: «**ذلك المحرر الإلكتروني الذي يثبت فيه موظف عام أو شخص مكلف بخدمة عامة، ما تم على يديه أو ما تلقاه من ذوي الشأن، وذلك طبقا للأوضاع القانونية وفي حدود سلطته واختصاصه**» [1]. كما تم تعريفه أيضا بأنه: «**السند الذي ينظمه أصحابه بطريقة إلكترونية ويصادق عليه الموظف العام، أو موظف التصديقات الذي من اختصاصه المصادقة عليه بطريقة إلكترونية طبقا للقانون، وأيضا بعد التحقق من توافر شروط معينة**» [2].

وعرفّ المشرع الجزائري العقد الرسمي من خلال المادة (324) من القانون المدني الجزائري على أنه: «**العقد الرسمي عقد**[3] **يثبت فيه موظف عام أو ضابط عمومي أو شخص مكلف بخدمة عامة، ما تم لديه أو ما تلقاه من ذوي الشأن وذلك طبقا للأشكال القانونية وفي حدود سلطته واختصاصه**».

تنقسم المحررات الرسمية إلى نوعين؛ محررات رسمية ينظمها الموظفون العموميون، كالأوراق الخاصة بالحالة المدنية والوثائق الرسمية القضائية كالأحكام والقرارات

---

(1)- **محمد محمد سادات**، مرجع سابق، ص 168.

(2)- **أحمد عزمي الحروب**، السندات الرسمية الالكترونية، دراسة مقارنة، دار الثقافة،2010، عمان، ص 77.

(3)- كان المشرع الجزائري قبل تعديل (1988) قانون رقم 88-14 المؤرخ في 16 رمضان 1408 الموافق 3 مايو 1988 يعدل ويتمم الأمر رقم 75-58 المؤرخ في 26 سبتمبر 1975 والمتضمن القانون المدني" يستعمل عبارة الورقة الرسمية، وبعد التعديل صار يستعمل مصطلح العقد الرسمي. ما يمكن قوله في هذا المقام، أن المشرع الجزائري لم يُصب في اعتماده لمصطلح العقد، إذ يعتبر العقد التصرف القانوني الذي يتم بتوافق إرادتين، في حين أن أداة إثباته التي يدون عليها هذا الاتفاق تدعى بالمحرر أو السند، فهو الوسيلة التي يمكن عن طريقها إثبات التعبير عن الإرادة، أي المحرر المدون فيه ما تم الاتفاق عليه. ولفظ " **Acte** " يطلق في لغة القانون الفرنسية على التصرف وأداة إثباته معا وهو العقد المكتوب، وقد تسرب هذا اللبس إلى لغة القانون العربية، كما فعل المشرع الجزائري في المادة (324) وما يليها من القانون المدني؛ عندما عبّر عن المحرر الرسمي والمحرر العرفي بالعقد، وهو تعبير خاطئ ، فأطلق لفظ "العقد" على التصرف ثم استعمله في أداة إثباته، فقيل "عقد رسمي" و " عقد عرفي" وقصد بذلك المحرر الرسمي والمحرر العرفي الذي يُعد لإثبات التصرف.

لمزيد من التفصيل راجع: **عربي باي يزيد**، العقود التوثيقية سندات تنفيذية على ضوء قانون الإجراءات المدنية والإدارية رقم 08-09، مجلة دفاتر السياسة والقانون، كلية الحقوق جامعة ورقلة، العدد 10 جانفي 2014، ص 132.

ومحاضر المنفذين، وكذا الوثائق الرسمية العامة كالقرارات الإدارية والقوانين والمعاهدات، وهذه المحررات الصادرة في شكل إلكتروني يمكن أن تصبغ عليها طابع الرسمية، لإمكانية توقيعها بواسطة توقيع إلكتروني مؤمن يصادق عليه الطرف الثالث الموثوق التابع للهيئة المصدرة. وقد تم هذا فعليا من خلال القانون (15-03) المتعلق بعصرنة العدالة، أين مكّن هذا القانون وزارة العدل من تسليم شهادات الجنسية والسوابق القضائية إلكترونيا، إلى جانب العديد من المشاريع المشابهة كاستخراج وثائق الحالة المدنية وبطاقة التعريف وجواز السفر البيومتريين، وإصدار بطاقات الشفاء وبطاقات السحب البريدي... وغيرها من المحررات الإلكترونية الرسمية... كل هذا في إطار تعزيز فكرة "الحكومة الإلكترونية".

أما النوع الثاني من المحررات الإلكترونية الرسمية، والتي يتدخل في إنشائها ضابط عمومي كالموثق والمحضر القضائي، فالمشرع الجزائري لم ينص صراحة لا في القانون المدني ولا في قانون التوثيق على إمكانية إنشاء محرر رسمي في شكل إلكتروني، ولعل ذلك راجع إلى خشية المشرع على هذه المعاملات من منظومة لم تستكمل بعد فترة التجربة.

وفي غياب تنظيم تشريعي للمحررات الرسمية الإلكترونية في الجزائر نستعرض التجربة الفرنسية في مجال تنظيمها.

اعترف المشرع الفرنسي بالمحرر الرسمي الإلكتروني من خلال المادة (1369) من القانون المدني الفرنسي، إذ نص على إمكانية إنشـــاء محـــرر رسمي على دعامة إلكترونية، وقبوله كدليل إثبات في حال ما توافرت في إعداده وحفظه الشروط المحددة من مرسوم صادر عن مجلس الدولة [1].

أصدر بعد ذلك مجلس الدولة الفرنسي مرسوم تحت رقم (973-2005) أين حدد من خلاله شروط إنشاء وحفظ المحررات الرسمية الإلكترونية وصورها للموثقين[2]. تنص المادة

)-1(Article 1369 du code civil français: «**L'acte authentique est celui qui a été reçu, avec les solennités requises, par un officier public ayant compétence et qualité pour instrumenter. Il peut être dressé sur support électronique s'il est établi et conservé dans des conditions fixées par décret en Conseil d'État. Lorsqu'il est reçu par un notaire, il est dispensé de toute mention manuscrite exigée par la loi ».** Modifié par Ordonnance n°2016-131 du 10 février 2016 – art 4.

)-2(Décret n° 2005-973 du 10 août 2005 modifiant le décret n° 71-941 du 26 novembre 1971 relatif aux actes établis par les notaires, JORF n°186 du 11 août 2005 page 13096 texte n° 34. https://www.legifrance.gouv.fr/

(16) من هذا المرسوم[1]، على أن يستعمل الموثق الذي يحرر عقد على دعامة إلكترونية نظام معالجة وإرسال للمعطيات مُرخص من قبل المجلس الأعلى للموثقين لضمان الأمان والثقة في محتوى المحرر.

كما اشترطت المادة (17)[2] من هذا المرسوم على الموثق وضع توقيعه الإلكتروني المؤمن كما هو محدد في المرسوم رقم (941-71) المتعلق بالمحررات المنشأة من طرف الموثقين المعدل بموجب المرسوم (973-2005).

تنص كذلك المادة (20 /1) من المرسوم (973-2005) على أنه إذا لم يحضر أحد أو كل الأطراف المتعاقدة أمام الموثق المعتمد فإنه يتم تلقي رضائهم وتوقيعاتهم [3]من قبل موثقين آخرين يحضرون أمامهم ويشاركون في تأسيس العقد.

ثم تنص الفقرة (2) من المادة نفسها، على أنه من الضروري لتأسيس العقد المذكور في المادة (16) أعلاه أن يتبادل الموثقون المعلومات المتعلقة برضا وأهلية الأطراف، لتلزم الفقرة (3) الموثقين من التحقّق من رضا وتوقيع الأطراف أو الأشخاص المتعاقدة، ثم يضعون

)-1(Art 16 du décret n° 71-941: **«Le notaire qui établit un acte sur support électronique utilise un système de traitement et de transmission de l'information agréé par le Conseil supérieur du notariat et garantissant l'intégrité et la confidentialité du contenu de l'acte.**
Les systèmes de communication d'informations mis en œuvre par les notaires doivent être interopérables avec ceux des autres notaires et des organismes auxquels ils doivent transmettre des données».
)-2(Art 17 du décret n° 71-941: **«L'acte doit être signé par le notaire au moyen d'un procédé de signature électronique sécurisée conforme aux exigences du décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique.**
Cette signature est apposée par le notaire dès l'acte établi, si besoin après réunion des annexes à l'acte.
Pour leur signature, les parties et les témoins doivent utiliser un procédé permettant l'apposition sur l'acte notarié, visible à l'écran, de l'image de leur signature manuscrite.
Lorsque l'acte doit contenir une mention manuscrite émanant d'une personne qui y concourt, le notaire énonce que la mention a été apposée dans le respect des conditions prévues au second alinéa de l'article 1108-1 du code civil».
)-3(Art 20 du décret n° 71-941: **«Lorsqu'une partie ou toute autre personne concourant à un acte n'est ni présente ni représentée devant le notaire instrumentaire, son consentement ou sa déclaration est recueilli par un autre notaire devant lequel elle comparaît et qui participe à l'établissement de l'acte. Cet acte porte la mention de ce qu'il a été ainsi établi. L'échange des informations nécessaires à l'établissement de l'acte s'effectue au moyen du système de transmission de l'information mentionné à l'article 16. Chacun des notaires recueille le consentement et la signature de la partie ou de la personne concourant à l'acte puis y appose sa propre signature. L'acte est parfait lorsque le notaire instrumentaire y appose sa signature électronique sécurisée ».**

توقيعهم الشخصي، لتنص الفقرة (4) والأخيرة على أن العقد يكتمل بوضع الموثق المعتمد توقيعه الإلكتروني المؤمن.

نستنتج من خلال نص المادة (20) من المرسوم (973-2005) أن المشرع الفرنسي وجد الحل لمسألة مهمة جدا؛ وهي إشكالية الحضور الفعلي والمادي للموثق أثناء ابرام العقود الرسمية الإلكترونية؛ إذ يعتبر شرط التواجد الفعلي للموثق جوهر فكرة الرسمية، وبذلك فقد أزال المشرع الفرنسي الغموض عن المحررات الرسمية الإلكترونية بوضعه منظومة تشريعية متكاملة ومُحكمة تأطّر كيفية إنشاء المحررات الرسمية الإلكترونية.

الفرع الثاني
عناصر حجية المحرر الرسمي الإلكتروني

إذا ما اكتسب المحرر الإلكتروني صفة الرسمية؛ كان حجة في ذاته ولا يجوز الطعن فيه إلا بالتزوير، مثله مثل المحرر الرسمي التقليدي[1]، وإعمالا لمبدأ التعادل الوظيفي بين المحررات الرسمية الإلكترونية والمحررات الرسمية التقليدية؛ تكون المحررات الرسمية الإلكترونية حجة على الناس كافة، سواء الأشخاص الموقعين عليها أو الغير **(أولا)**، إضافة إلى حجية البيانات الواردة فيها **(ثانيا)**، وكذلك تكون حجة من ناحية سلامتها المادية **(ثالثا)**، وسيتم التفصيل في هذه النقاط الثلاثة تباعا فيما يلي.

أولا: حجية المحررات الرسمية الإلكترونية بالنسبة للأشخاص

يُستفاد من نص المادة (324 مكرر 5) من القانون المدني الجزائري والتي تنص على أنه: «**يعتبر ما ورد في العقد الرسمي حجة حتى يثبت تزويره ويعتبر نافذا في كامل التراب الوطني**»، وتنص المادة (324 مكرر 6) على أنه: «**يعتبر العقد الرسمي حجة لمحتوى الاتفاق المبرم بين الأطراف المتعاقدة وورثتهم وذوي الشأن...**»، وكذلك محتوى المادة (324

(1)- **محمد صبري السعدي**، الواضح في شرح القانون المدني (الإثبات في المواد المدنية والتجارية)، ط1، دار الهدى، الجزائر، 2011، ص 57؛ **جديد حنان**، السندات الرسمية الإلكترونية، مجلة الحقوق والعلوم الإنسانية، المجلد 08، العدد 01، 2015، ص 253.

مكرر 7) والتي تقضي بأن: «**يعتبر العقد الرسمي حجة بين الأطراف حتى ولو لم يعبر فيه إلا ببيانات على سبيل الإشارة، شريطة أن يكون لذلك علاقة مباشرة مع الإجراء...**».

يتضح من فحوى هذه المواد أن المحرر الرسمي له حجة قانونية بالنسبة لأطرافه وورثتهم وتمتد لتشمل الغير، فيعتبر حجة على الناس كافة بما دون فيه، فلا يمكن إنكار ما ورد فيه من بيانات تحقق الموظف العمومي من صحتها أو وقعت من ذوي الشأن في حضوره إلا عن طريق التزوير[1].

وبتطبيق القواعد العامة للمحررات العادية على المحررات الإلكترونية، فإن هذه الأخيرة ومتى توافرت على الشروط السابق ذكرها، تكتسب صفة الرسمية وتكون حجة على الكافة بمن فيهم الأشخاص الذين تحمل توقيعاتهم، وعلى خلفائهم العامين والخاصين، وعلى الغير كذلك وفقا للمواد (324 مكرر 5 و6 و7) المذكورة أعلاه.

بناء على المادة (324 مكرر 5) المذكورة أعلاه وكذلك المادة (31) من القانون (06-02) المعدل والمتمم يتضمن تنظيم مهنة الموثق[2] والتي تنص على: «**تسلم النسخة الممهورة بالصيغة التنفيذية للعقد التوثيقي وفقا للتشريع المعمول به، ويسري عليها ما يسري على تنفيذ الأحكام القضائية**»، وعليه تتوفر المحررات الرسمية سواء العادية أو الإلكترونية (وفقا لمبدأ التعادل الوظيفي) على القوة التنفيذية لاستيفاء الحقوق دون الحاجة لاستصدار حكم قضائي، وذلك عن طريق الحصول على نسخة تنفيذية ممهورة بالصيغة التنفيذية وفقا للمادة (602) من قانون الإجراءات المدنية والإدارية[3]، والتي ورد نصها كالآتي: «**لكل مستفيد من سند تنفيذي، الحق في الحصول على نسخة ممهورة بالصيغة التنفيذية المنصوص عليها في المادة 601 أعلاه، تسمى " النسخة التنفيذية ". ولا تسلم إلا للمستفيد شخصيا أو لوكيل عنه بوكالة خاصة. يمهر**

---

(1)- **عبد الرزاق أحمد السنهوري**، الوسيط في شرح القانون المدني الجديد 2، نظرية الالتزام بوجه عام، آثار الالتزام، دار النهضة العربية، القاهرة، 1968، ص 154.

(2)- قانون رقم 06-02 مؤرخ في 21 محرم عام 1427 الموافق 20 فبراير سنة 2006 يتضمن تنظيم مهنة الموثق، ج.ر.ع 14 صادر بتاريخ 08 مارس 2006 معدل ومتمم.

(3)- قانون رقم 08-09 مؤرخ في 18 صفر عام 1429 موافق 25 فبراير سنة 2008 يتضمن قانون الإجراءات المدنية والإدارية، ج. ر. ع 21 الصادر بتاريخ 23 أفريل 2008.

ويوقع على النسخة التنفيذية رئيس أمناء الضبط أو الضابط العمومي، حسب الحالة، وتحمل عبارة " نسخة تنفيذية مطابقة للأصل " وتختم بالختم الرسمي للجهة التي أصدرته».

ثانيا: حجية المحررات الرسمية الإلكترونية بالنسبة للبيانات الواردة فيها

تنقسم البيانات الواردة في المحررات الرسمية الإلكترونية إلى قسمين؛ بيانات يلحقها وصف الرسمية ولا يجوز الطعن فيها إلا بالتزوير، وبيانات أخرى لا يلحقها وصف الرسمية ويجوز إثبات عكسها وفقا للقواعد العامة.

1- البيانات التي لا يجوز الطعن في حجيتها إلا بالتزوير:

تشمل هذه البيانات نوعين من الوقائع: نوع يدونها الضابط العمومي أو المكلف بخدمة عامة بنفسه؛ كتأكده من شخصية الأطراف إما بشهادة شاهدين تحت مسؤوليتهما أو بمستند رسمي كبطاقات التعريف وجوازات السفر، ورخص السياقة، وكذا التأكد من توقيعاتهم، إثبات تاريخ المحرر، مكان التوثيق...

والنوع الثاني من البيانات يتمثل في الوقائع التي قام بها ذوو الشأن أمامه، أي ما عاينه الموظف العام أو الضابط العمومي أو ما سمعه بنفسه من وقائع مادية وقعت أمامه، كدفع أو قبض الثمن إذا كان واجب الدفع بمعاينة وأمام الضابط العمومي [1].

ولأهمية هذه البيانات تتطلب التشريعات وجوب حضور الأطراف أمـــام موظف عمومي، ولأن الأطراف لا يجمعهم مجلس عقد واحد، نص المشرع الفرنسي في المادة (20) من المرسوم (973-2005) في حال إبرام محرر رسمي إلكتروني على ضرورة تدخل أكثر من موثق لتلقي بيانات الأطراف المختلفة.

---

(1)- محمد حزيط، الإثبات في المواد المدنية والتجارية في القانون الجزائري، دار هومة، الجزائر، 2017، ص 80؛ **عبد الرزاق أحمد السنهوري**، مرجع سابق، ص154.

وعليه؛ لا يجوز الطعن في هذه البيانات إلا بالتزوير لأن التشكيك فيها يزعزع الثقة بالموظف العام أو الضابط العمومي [1].

2- البيانات التي يجوز إثبات عكسها وفقا للقواعد العامة في الإثبات:

تتمثل هذه البيانات في البيانات الصادرة من ذوي الشأن على مسامع الضابط العمومي أو الموظف العام والتي حصلت دون حضوره، فيقوم بتدوينها على مسؤوليتهم ولا تلحقها صفة الرسمية؛ كإقرار البائع باستلام الثمن والمشتري باستلام المبيع، فالموظف العام هنا يثبت واقعة الإدلاء بالإقرار، وتثبت له صفة الرسمية دون المساس بصحة مضمونه فلا تثبت لها الحجية[2]، ويجوز إثبات عكسها لمن له مصلحة بالطرق العادية وفقا للقواعد العامة في الإثبات دون الحاجة لسلوك طريق الطعن بالتزوير.

ومن تطبيقات المحكمة العليا في هذا الشأن، المبدأ المكرس في القرار الصادر عنها بتاريخ (2000/03/29) ملف رقم (190541) الذي جاء فيه ما يلي: «إذا كانت حجية الورقة الرسمية في الإثبات هي حجة على الناس كافة، أي فيما يتعلق بالمتعاقدين وبالنسبة للغير معا. فإنه يجب التفرقة بين الوقائع التي أثبتها الموثق مما جرى تحت سمعه وبصره والتي فيها مساس بأمانة الموثق وهذه حجيتها مطلقة ولا يجوز إنكارها إلا عن طريق الطعن فيها بالتزوير. أما الوقائع التي ينقلها ذوي الشأن فيجوز الطعن فيها عن طريق إثبات عكسها دون حاجة إلى الطعن في الورقة ذاتها بطريق التزوير» [3].

---

(1)- نظم المشرع الجزائري الادعاء بالتزوير في المحررات الرسمية في المواد 179-188 من القانون 08-09 المتضمن قانون الإجراءات المدنية والإدارية، وكذلك جرم الفعل بناء على المواد 214-218 من الأمر رقم **66- 156** مؤرخ في 18 صفر 1386 الموافق 08 جوان سنة 1966، يتضمن قانون العقوبات، ج.ر.ع 49 صادر بتاريخ 11 جوان 1966، معدل ومتمم.

(2)- **محمد صبري السعدي**، مرجع سابق، ص 54؛ **تامر محمد سليمان الدمياطي**؛ مرجع سابق، ص 738؛ **محمد محمد السادات**، حجية المحررات الموقعة إلكترونيا في الاثبات " دراسة مقارنة"، مرجع سابق، ص 239.

(3)- قرار رقم 190541 المؤرخ في 2000/03/29 صادر عن الغرفة العقارية، منشور بالمجلة القضائية للمحكمة العليا، العدد الأول لسنة 2000، ص 154.

وكذلك القرار رقم (20264) المؤرخ في (27 سبتمبر 2000) الصادر عن الغرفة العقارية بالمحكمة العليا الذي جاء فيه ما يلي: «حيث أن العقد التوثيقي يتضمن نوعين من البيانات: البيانات التي تتعلق بالوقائع التي يباشرها الموثق نفسه أو الوقائع المادية التي يقوم بها الأطراف أمام الموثق التي يعاينها، وهذه البيانات تكون حجة حتى يطعن فيها بالتزوير. أما البيانات المتعلقة بالتصريحات والاتفاقات التي يتلقاها الموثق من الأطراف، فتكون حجة إلى أن يثبت عكسها. حيث أن قضاة المجلس الذين سمحوا بإثبات عكس ما تضمنه عقد الشهرة المحتج به من طرف الطاعن فيما يخص التصريحات التي أدلوا بها للموثق لم يخالفوا أحكام المادة (324 مكرر 5) من القانون المدني الجزائري، ذلك أن التصريح الشرفي المدلى به للموثق من طرف الطاعن حول حيازة القطعة الأرضية المذكورة مساحتها وحدودها في عقد الشهرة يمكن أن يدحضها من ينازع في محتوى هذا التصريح بالدليل العكسي ودون الحاجة إلى الطعن بالتزوير في عقد الشهرة»[1].

ثالثا: حجية المحررات الرسمية الإلكترونية من حيث صدورها ممن وقعها وسلامتها المادية

يعد المحرر الرسمي الإلكتروني حجة بصدوره ممن يحمل توقيعاتهم الإلكترونية، ويستوي في ذلك الموظف العام وكذا أطراف المحرر، وعليه تثبت الحجية لواقعة ارتباط التوقيع الإلكتروني بالمحرر دون الحاجة للإقرار به، وعلى من يشكك في صدور المحرر من الأشخاص الذي يحمل توقيعاتهم إلا أن يطعن بالتزوير في هذه التوقيعات [2].

أما من ناحية قرينة السلامة المادية للمحرر الرسمي، فبتطبيق القواعد العامة للإثبات على المحررات الرسمية الإلكترونية؛ وجب خلو مظهرها من أي تغيير في محتواها بالمحو أو التعديل أو الكشط أو التحشير وغير ذلك من العيوب المادية.

غير أنه وإن كان بإمكان القاضي التحقق من السلامة المادية للمحرر الرسمي العادي وذلك لطبيعته المادية، فإن الأمر على خلاف ذلك بالنسبة للمحرر الرسمي الإلكتروني ذي

(1)- قرار رقم 20264 مؤرخ في 27 سبتمبر 2000، صادر عن الغرفة العقارية، منشور في مجلة الاجتهاد القضائي للمحكمة العليا، الجزء الثاني، لسنة 2004، ص 139.

(2)- **محمد حزيط**، مرجع سابق، ص 73؛ **بلحاج بالخير**، مرجع سابق، ص 368.

الطبيعة غير المادية والتي لا تتيح للقاضي التحقق من قرينة السلامة المادية إلا إذا استعان بذوي الخبرة بالوسائل الفنية والتقنية التي تتيح كشف هذه العيوب للوقوف على مدى صحة المحرر الرسمي الإلكتروني [1].

الفرع الثاني
حجية صور المحررات الرسمية الإلكترونية

إن الصـــورة المأخوذة للمحررات التقليدية تكون في شكل ورقي للطبيعة الماديـــة للدعامة، أما بخصوص المحررات الإلكترونية فهنا يثار التساؤل عن طبيعة الصور المأخوذة عنها.

يرى بعض الفقهاء[2]، ضرورة التفرقة بين المحررات الإلكترونية البحتة والمحررات الإلكترونية الجزئية؛ فالمحررات الإلكترونية البحتة تكون في حالة الكتابة المثبتة على دعامة إلكترونية، وتكون وسيلة إظهارها أيضًا دعامة إلكترونية، وفي هذه المحررات يلتقي أصل المحرر بالصورة بل يختلطان على وجه يصعب أن يتم فيه الفصل بينها فصلا دقيقًا.

فالبيانات المثبتة على دعامة إلكترونية تثبت بطريقة تضمن سلامتها وصحة التوقيع عليها منذ تدوينها لأول مرة ومن ثم تتحقق لها فكرة الأصل. كما أن دقة مطابقة مخرجات الجهاز غير الورقية لما هو مثبت داخل الجهاز يسمح بأن تمتد لهذه المخرجات فكرة الأصـــل، وقد اصطلح على هذا النوع من المحررات تسمية المحررات الإلكترونية الكاملة.

---

(1)- صبحي محمد أمين، الطبيعة القانونية لجريمة التزوير في المحررات، مجلة القانون العام الجزائري والمقارن، العدد06، سنة 2017، ص 53.

(2)- محمد محمد أبو زيد، نحو اتساق القواعد الفرعية في الاثبات مع مبدأ الاعتراف التشريعي بحجية الكتابة الإلكترونية، دار النهضة العربية، القاهرة، 2006، ص 31 وما يليها؛ **أزرو محمد رضا**، إشكالية إثبات العقود الإلكترونية – دراسة مقارنة– ، رسالة مقدمة لنيل شهادة الدكتوراه في العلوم، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، 2016، ص 127.

أما المحررات الإلكترونية الجزئية، فهي المحررات التي تكون فيها الكتابة مثبتة على دعامة إلكترونية ولكن يتم إظهارها أو استخراجها على دعامة ورقية، فتلك المحررات يتم الحصول منها على صورة منسوخة من المحرر الإلكتروني على الورقة [1].

بناء على هذا الرأي، يجب عدم التمييز بين الأصل والصورة في حالة المحررات الإلكترونية البحتة، والإبقاء على التمييز بين الأصل والصورة في حالة المحررات الإلكترونية الجزئية.

إلا أن هناك بعض من الفقه [2]؛ من شكك في هذا التقسيم؛ على أساس أن التفرقة السابقة اعتمدت التمييز بين المحررات الإلكترونية بناء على الصورة المأخوذة، فقللت من قيمة المحرر الإلكتروني بوصفه محرر إلكتروني جزئي لمجرد طباعته على ورق، والمحرر الإلكتروني كما بينا سابقا متى نشأ أو أرسل أو حفظ بوسيلة إلكترونية أصبح محررا إلكترونيا لا ينتقص منه طباعة صورة له في شكل ورقي، وهو ما استقرت عليه جميع التشريعات في تعريفها للمحرر الإلكتروني.

فالنصوص التشريعية لم تعط حجية أعلى للمحررات الإلكترونية الكاملة عن تلك المعطاة للمحررات الإلكترونية الجزئية، ولم تمنح الصورة الإلكترونية للمحرر الإلكتروني الكامل حجية أعلى من تلك الممنوحة للصورة الورقية للمحرر الإلكتروني الجزئي.

وقد أقر المشرع المصري بإمكانية إصدار صورة ورقية من المحرر الرسمي الإلكتروني وذلك من خلال المادة (16) من القانون (15 لعام 2004) المتعلق بالتوقيع الإلكتروني المصري والتي تنص على أن: «**الصورة المنسوخة على الورق من المحرر الإلكتروني الرسمي حجة على الكافة بالقدر الذي تكون فيها مطابقة لأصل هذا المحرر، وذلك ما دام المحرر الإلكتروني الرسمي والتوقيع الإلكتروني موجودين على الدعامة الإلكترونية**».

---

(1)- محمد محمد أبو زيد، المرجع نفسه، ص 34.

(2)- محمد محمد سادات مرزوق، حجية أصل المحررات الرسمية الإلكترونية وصورها في الإثبات -دراسة مقارنة-، الفكر الشرطي، المجلد 25، العدد 98، يوليو 2016، ص ص 232- 233.

نلاحظ من خلال هذا النص، أن المشرع المصري أقر بإمكانية إصدار صورة ورقية للمحرر الإلكتروني الرسمي دون أن يتطرق لإمكانية إصدارها في صورة إلكترونية. كما اشترط لاكتسابها حجية الأصل أن تكون مطابقة له، مع ضرورة وجود المحرر الإلكتروني الرسمي والتوقيع الإلكتروني على الدعامة الإلكترونية.

أما عن المشرع الفرنسي، فقد تولى تنظيم النصوص الخاصة بطبيعة صور المحررات بنوعيها (التقليدية والإلكترونية) من خلال المرسوم (973-2005) المتعلق بالمحررات المنشأة من طرف الموثقين، حيث تنص المادتين (34 و37) منه على الأحكام الخاصة بتكوين صورة إلكترونية من المحرر، سواء أكان هذا المحرر ورقيا أو إلكترونيا، فيمكن للموثق أن يقدم صورة إلكترونية لأصل محرر ورقي رسمي أو محرر إلكتروني رسمي، كما يمكنه أن يصدر صورة إلكترونية لمحرر رسمي ورقي بشرط توافر مجموعة من الشروط التي سنبينها في النقطة الموالية.

أولا: الشروط الواجب توافرها لإصدار صورة ورقية من محرر إلكتروني

تنص المادة (34 فقرة 1 و2 و3 و4)[1]من المرسوم الفرنسي (973-2005) المتعلق بالمحررات المنشأة من طرف الموثقين على مجموعة من الشروط لإصدار نسخة ورقية من محرر إلكتروني، وتتمثل هذه الاشتراطات في:

- أن تكون النسخة مقروءة وثابتة على ورق يضمن جودة الحفظ؛
- أن ترقم كل صفحة من صفحات النسخة المصدرة؛

) -1(Article 34 du décret n° 71-941 du 26 novembre 1971 relatif aux actes établis par les notaires: **«les copies exécutoires et les copies authentiques sont établies de façon lisible et indélébile sur un papier d'une qualité offrant toute garantie de conservation.**
Elles respectent les paragraphes et les alinéas de la minute. Chaque page de texte est numérotée, le nombre de ces pages est indiqué à la dernière d'entre elles.
Chaque feuille est revêtue du paraphe du notaire à moins que toutes les feuilles ne soient réunies par un procédé empêchant toute substitution ou addition ou qu'elles ne reproduisent les paraphes et signatures de la minute.
La signature du notaire et l'empreinte du sceau sont apposées à la dernière page et il est fait mention de la conformité de la copie exécutoire ou de la copie authentique avec l'original… »

- أن يوقع الموثق بالأحرف الأولى على كل صفحة على الأقل، ما لم يتم تجميع كل الصفحات بواسطة إجراءات تمنع حدوث أي تحريف أو إضافة بها؛
- أن يذكر الموثق مطابقة هذه الصورة مع أصل المحرر الإلكتروني بعد أن يضع توقيعه وختمه الخاص على الصفحة الأخيرة.

ثانيا: الشروط الواجب توافرها لإصدار صورة إلكترونية من محرر إلكتروني

تنص على هذه الشروط المادة (2/37) من المرسوم (973-2005) السالف الذكر[1]، وتتمثل في:

- تاريخ إصدار النسخة؛
- وضع الموثق توقيعه الإلكتروني المؤمن، وصورة من ختمه الخاص بواسطة الماسح الضوئي؛
- إشارة من الموثق تفيد بمطابقة الصورة الإلكترونية للأصل.

ثالثا: إصدار نسخة إلكترونية من محرر ورقي

أشارت المادة (1/37) من المرسوم (973-2005) السالف الذكر، إلى أنه مثلما للموثق إمكانية إصدار صور ورقية من محررات إلكترونية، فإن له كذلك أن يصدر صور إلكترونية من محررات ورقية شرط أن يتم ذلك بواسطة ظروف ونظام إلكتروني يضمن تطابقهما [2].

إضافة إلى ما سبق ذكره، سمحت الفقرة الأخيرة من المادة (37) من المرسوم (973-2005) السالف الذكر، بتسليم هذه الصورة الإلكترونية للمحرر الرسمي بطريقة إلكترونية، شرط أن يتم ذلك في ظروف تضمن سلامة بيانات النسخة المصدرة، سرية عملية النقل وخصوصيتها، مع إمكانية تحديد هوية المرسل والمرسل إليه [3].

)-1(Article 37/2 du décret n° 71-941 du 26 novembre 1971 relatif aux actes établis par les notaires**: «…Le notaire qui délivre une copie sur support électronique y mentionne la date et y appose sa signature électronique qualifiée. La copie authentique comporte en outre l'image de son sceau. Mention est portée sur la copie délivrée de sa conformité à l'original…** »

)-2(Article 37/1 du décret n° 71-941 du 26 novembre 1971 relatif aux actes établis par les notaires: **«Le notaire peut procéder à la copie sur support électronique d'un acte établi sur support papier après avoir utilisé un système de numérisation dans des conditions garantissant sa reproduction à l'identique…»**

)-3(Article 37/3 du décret n° 71-941 du 26 novembre 1971 relatif aux actes établis par les notaires**: «Les copies exécutoires et copies authentiques peuvent être transmises par voie électronique dans des conditions=**

بالنسبة للمشرع الجزائري؛ فإنه لم يشر لا في القانون المدني ولا في القانون الخاص بالتوقيع والتصديق الإلكترونيين؛ لإمكانية إصدار نسخ؛ سواء ورقية أو إلكترونية؛ للمحررات الإلكترونية، ليكتفي بما هو مقرر في القواعد العامة في أحكام القانون المدني والتي تخص صور المحرر على الورق بشكل عام، لنجد أنفسنا كل مرة أمام فراغ تشريعي وجب على المشرع الجزائري سدّه بالاستفادة من تجارب التشريعات التي سبقته في تنظيم هذه المعاملات.

أما عن حجية الصورة الإلكترونية للمحرر الرسمي الإلكتروني، وفي ظل هذا الفراغ القانوني؛ نقوم بتطبيق القواعد العامة في الإثبات والمقررة بشأن حجية صور المحررات الرسمية التقليدية ونص المشرع الجزائري هنا على حالتين:

الحالة الأولى: حجية الصورة في حال كان الأصل موجودا

تنص المادة (325) من القانون المدني الجزائري، على أنه إذا كان أصل المحرر الرسمي موجودا فإن صورته تكون لها ذات الحجية المقررة للأصل، وتعتبر الصورة مطابقة للأصل ما لم ينازع أحد الطرفين في ذلك، وفي حال نشوب نزاع تراجع الصورة على الأصل[1].

الحالة الثانية: حجية الصورة في غياب الأصل

هي الحالة التي تنص عليها المادة (326)[2] من القانون المدني الجزائري، ففي حال كان أصل المحرر الرسمي غير موجود، نتيجة لفقد بسبب ضياع أو سرقة أو حريق أو تلف أو غيرها وبقيت الصورة فقط، فإنه يتعين التفرقة بين ثلاث فروض:

=garantissant l'intégrité de l'acte, la confidentialité de la transmission, l'identité de l'expéditeur et celle du destinataire».

(1)- تنص المادة 325 ق.م.ج: «**إذا كان أصل الورقة الرسمية موجودا، فإن صورتها الرسمية خطية كانت أو فوتوغرافية تكون حجة بالقدر الذي تكون فيه مطابقة للأصل.**

وتعتبر الصورة مطابقة للأصل ما لم ينازع في ذلك أحد الطرفين، فإن وقع تنازع ففي هذه الحالة تراجع الصورة على الأصل».

(2)- تنص المادة 326 ق م ج: «**إذا لم يوجد أصل الورقة الرسمية كانت الصورة حجة على الوجه الآتي:**

- **يكون للصور الرسمية الأصلية تنفيذية كانت أو غير تنفيذية حجية الأصل متى كان مظهرها الخارجي لا يسمح بالشك في مطابقتها للأصل.** =

أ- إذا كانت الصورة المقدمة مأخوذة عن المحرر الرسمي مباشرة، تكون لها حجية الأصل متى كان مظهرها الخارجي لا يسمح بالشك في مطابقتها للأصل من حيث شكلها ومضمونها.
ب- تكون للصورة الرسمية المأخوذة عن الصورة الرسمية الأصلية نفس حجية الصورة الأصلية ما لم ينازع فيها أحد الطرفين، ويجوز لكل من الطرفين أن يطلب مراجعتها على الصورة الأصلية المأخوذة منها. فإن فقدت هذه الأخيرة فإن الصورة الرسمية المأخوذة عنها لا تكون لها حجية في الإثبات إلا على سبيل الاستئناس تبعا للظروف [1].
ت- أما عن الصورة الرسمية للصور المأخوذة من الصورة الأصلية فلا حجية لها في الإثبات، ولا يعتد بها إلا على سبيل الاستئناس تبعا للظروف.

نتساءل في الأخير عن سبب منع المشرع الجزائري التعامل بأي سلعة أو خدمة تتطلب عقد رسمي على الرغم من إصداره للقانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين، واحتوائه على كل سبل إنشاء تواقيع إلكترونية موصوفة، وكذا شهادات التصديق الإلكتروني، واعتماده على تقنيات التشفير والحفظ الإلكتروني... وعلى كل ما يُمكن من إصدار محررات رسمية إلكترونية، فإن كان السبب راجع إلى تخوّف المشرع الجزائري من طريقة إعداد هذه المحررات الرسمية الإلكترونية نظرا لخطورتها وتعقد إجراءاتها وقيمتها المالية، فبإمكانه تعزيز المنظومة التشريعية بنصوص وتقنيات تضفي الثقة والاستقرار في المعاملات الإلكترونية، والمحررات المثبتة لها بكافة أنواعها مستأنسا في ذلك بما سبقتنا إليه التشريعات الأخرى التي برعت في تنظيمه كحال المشرع الفرنسي الذي وضع تنظيما متكاملا لعملية توثيق المحررات الإلكترونية بداية من كيفية إنشائها وفقا لنظام معلومات خاص، وإثبات تاريخها، وكيفية التوقيع عليها، انتهاء بكيفية حفظها.

=- ويكون للصور الرسمية المأخوذة عن الصور الأصلية الحجية ذاتها ولكن يجوز في هذه الحالة لكل من الطرفين أن يطلب مراجعتها على الصورة الأصلية التي أخذت منها.

- أما ما يؤخذ من صور رسمية للصورة المأخوذة من النسخ الأولى فلا يعتد به إلا لمجرد الاستئناس تبعا للظروف».

(1)- محمد صبري السعدي، مرجع سابق، ص55؛ **محمد حزيط**، مرجع سابق، ص 85.

المطلب الثاني
القيمة الثبوتية للمحررات العرفية الإلكترونية

ينقسم المحرر العرفي؛ سواء التقليدي أو الإلكتروني إلى قسمين؛ محرر عرفي مُعد للإثبات وهي المحررات الموقعة من ذوي الشأن، ولا تتوفر فيها مقومات المحـــررات الرسمية، أي لا تتطلب شكلية محددة لإنشائها [1]، وتعتبر هذه المحررات حجة على من صدرت منهم إذا ما استكملت شرطي الكتابة والتوقيع.

ولا يشترط في تحرير المحرر العرفي اعتماد لغة معينة، فهو يخضع لمبدأ الحرية في تحريره ما عدا ما استثناه القانون، إلا أن التوقيع يعتبر الشرط الجوهري في المحرر العرفي المعد للإثبات، لأنه يثبت قبول الموقع لما وقعه [2].

أما النوع الثاني من المحررات الإلكترونية العرفية؛ فهي تلك المحررات غير المعدة سلفا للإثبات؛ أي لم يُقصد من تحريرها استعمالها في الإثبات، فهذا النوع من المحررات خال من التوقيع على الرغم من وجوده في بيئة افتراضية. وتتمثل صور هذه المحررات في كل من الرسائل المرسلة عبر الوسائل الإلكترونية (رسائل البريد الإلكتروني، رسائل الهاتف المحمـــول، رسائل الفاكس والتلكس وكذا الدفاتر التجارية الإلكترونية)

وعليه سنحاول من خلال هذا المطلب التطرق لكل من حجية المحررات العرفية الإلكترونية المُعدّة للإثبات **(فرع أول)**، ثم لحجية المحررات الإلكترونية غير المُعدّة للإثبات **(فرع ثان)**.

)-1(**GAUTRAIS Vincent,** Le contrat électronique international, 2e édition revue, DELTA, Beyrouth, 2003, p104.
)-2(**CAPRIOLI Éric,** Écrit et Preuve Électronique dans la loi nº2000-230 du 13mars 2003, la semaine juridique, jurisclasseur périodique, nº2, 2000. p8.

الفرع الأول
حجية المحررات العرفية الإلكترونية المُعدّة للإثبات

أقرت أغلبية التشريعات التي درسناها سابقا [1]؛ للمحررات العرفية الإلكترونية المُعدّة للإثبات بذات الحجية القانونية للمحررات العرفية التقليدية المُعدّة للإثبات في حال ما استوفت الشروط العامة المتطلبة لصحة المحررات التقليدية، وكذا المتطلبات الفنية والتقنية اللازمين للكتابة والتوقيع الإلكترونيين.

إلا أن هناك من الفقه من ينتقد هذه المساواة المطلقة؛ على أساس أن التوقيع الإلكتروني الذي يعتبر أهم عناصر المحرر الإلكتروني هو في الأصل على مستويات متعددة من الأمـــان؛ لذا تختلف حجية المحررات الإلكترونية في الإثبات على حسب حجية التوقيع الإلكتروني الممهورة به، وعليه سنحاول من خلال هذا الفرع توضيح الرأي القائل بالمساواة المطلقة في الحجية بين المحررات التقليدية والمحررات الإلكترونية **(أولا)**، والرأي الثاني الذي يرى بعدم المساواة في حجية بين المحررات الإلكترونية والمحررات التقليدية **(ثانيا)**.

أولا: المساواة المطلقة بين المحرر العرفي الإلكتروني والمحرر العرفي الورقي

يترتب على إعمال مبدأ المساواة بين المحررات العرفية الإلكترونية والمحررات العرفية التقليدية من حيث الحجية في الإثبات؛ إخضاع المحررات العرفية الإلكترونية لذات القيود التي تخضع لها المحررات العرفية التقليدية، والتي تتمثل أساسا في ثلاث نواحي: من حيث صدورها ممن وقع عليها (مصدرها)، ومن حيث قوة البيانات المدونة فيها، ومن حيث التاريخ الذي تحمله.

وعليه سنتناول حجية المحررات العرفية الإلكترونية من حيث هذه الجوانب الثالثة تباعا.

---

(1)- نص على حجية المحررات الإلكترونية في الاثبات قانون اليونسترال بشأن التجارة الإلكترونية لعام (1996) من خلال المادة (9 فقرة 02) منه، والمشرع الجزائري من خلال المادة (323 مكرر 1) من القانون المدني الجزائري، والمشرع الفرنسي من خلال المادة (1366) من القانون المدني الفرنسي، والمشرع الأردني من خلال المادة (13) من قانون البيانات الأردني، وكذا المشرع المصري من خلال المادة (15) من قانون التوقيع الإلكتروني.

1- حجية المحرر العرفي الإلكتروني من حيث صدوره ممن وقع عليه:

تنص المادة (327) من القانون المدني الجزائري على: «**يعتبر العقد العرفي صادرا ممن كتبه أو وقعه أو وضع عليه بصمة إصبعه ما لم ينكر صراحة ما هو منسوب إليه، أما ورثته أو خلفه فلا يطلب منهم الإنكار ويكفي أن يحلفوا يمينا بأنهم لا يعلمون أن الخط أو الإمضاء أو البصمة هو لمن تلقوا منه هذا الحق...**». يستفاد من هذه المادة أن المحرر العرفي يعتبر حجة على من صدر منه، سواء بالنسبة لمن كتبه أو وقعه، أو وضع عليه بصمة إصبعه، متى اعترف به ولم ينكره صراحة؛ كأن يعرض عليه ويسكت ولم ينكر صراحة صدوره منه.

إن اعتراف صاحب التوقيع بصدور المحرر منه، سواء كان هذا الاعتراف صريحا أو ضمنيا، يجعل من المحرر صادرا منه واعتبر التوقيع توقيعه، ليصبح المحرر العرفي من حيث صدوره ممن وقع عليه في قوة المحرر الرسمي، ولا يجوز لصاحب التوقيع أن يعود بعد ذلك بالإنكار إلا أن يطعن بالتزوير، على اعتبار أن التسليم بصحة التوقيع لا يتعارض مع ادعائه بتزوير بعض بياناتها [1].

أما إذا أنكر من نُسب إليه المحرر صدوره منه، يفقد المحرر حجيته بصفة مؤقتة، لغاية الفصل في ذلك من طرف المحكمة. ويقع عبء إثبات صدوره من صاحب التوقيع على من يتمسك بالمحرر، وله أن يطلب إحالة المحرر على التحقيق، فتجري المحكمة تحقيقا عن طريق مضاهاة الخطوط [2]، وإذا أثبت التحقيق أنه هو من وقع عليه صار المحرر العرفي كالمحرر الرسمي، ولا يجوز له الطعن فيه إلا بالتزوير.

---

(1)- عبد الرزاق أحمد السنهوري، مرجع سابق، ص 189؛ **محمد حزيط**، مرجع سابق، ص 94؛ **تامر محمد سليمان الدمياطي**، مرجع سابق، ص 764.

(2)- تنص المادة (164) ق.إ.م.إ على: «**تهدف دعوى مضاهاة الخطوط إلى إثبات أو نفي صحة الخط أو التوقيع على المحرر العرفي.**

يختص القاضي الذي ينظر في الدعوى الأصلية، بالفصل في الطلب الفرعي لمضاهاة الخطوط المتعلقة بمحرر عرفي.

يمكن تقديم دعوى مضاهاة الخطوط للمحرر العرفي كدعوى أصلية أمام الجهة القضائية المختصة». كما تنص المادة (165) ق.إ.م.إ على: «**إذا أنكر أحد الخصوم الخط أو التوقيع المنسوب إليه، أو صرح بعدم الاعتراف بخط أو توقيع الغير، يجوز للقاضي أن يصرف النظر عن ذلك إن رأى أن هذه الوسيلة غير منتجة في الفصل في النزاع.** =

ولا يجوز أن يصدر الإنكار من الخلف أو الدائن لأن التوقيع غير صادر منهما، أما إذا حدث التمسك بالمحرر بعد وفاة صاحب التوقيع، فإنه يكون حجة في مواجهة الخلف الخاص والدائن والوارث والموصى له. ومع ذلك يجوز لأي من هؤلاء أن يتمسك بعدم صدور المحرر ممن وقعه لا عن طريق إنكار التوقيع؛ بل عن طريق الدفع بالجهالة، أي الدفع بأنهم لم يعلموا بصدور التوقيع من الشخص المنسوب إليه، ويطلب منهم الحلف بأن الخط أو الإمضاء أو البصمة ليست لمن تلقوا منه الحق [1]، فإن أدوا اليمين زال عن المحرر العرفي حجيته مؤقتا إلى غاية إثبات العكس[2].

بناءً على ما سبق شرحه، واستنادا لعدم وجود قواعد خاصة تنظم المحرر العرفي الإلكتروني، وكذا إعمالا لمبدأ التعادل الوظيفي بين المحررات العرفية التقليدية والمحررات العرفية الإلكترونية، فالمحرر العرفي الإلكتروني يعتبر حجة على من صدر منه شرط الاعتراف به أو عدم إنكاره. لكن ونظرا للطبيعة التقنية الخاصة بالمحرر الإلكتروني؛ لا يمكن أن نتصور إنكار الخط، لأن الخط في هذه الحالة لا يكون باليد، بل بواسطة الحاسوب. فهنا لا يمكن تصور اللجوء إلى مضاهاة الخطوط، وبالتالي فإن إنكار الشخص يقتصر فقط على توقيعه الإلكتروني.

غير أنه في حال إنكار من نُسب إليه التوقيع الإلكتروني، فيفقد المحرر العرفي الإلكتروني حجيته مؤقتا إلى غاية إثبات العكس، لِيقع على من ادعى بصحة هذا التوقيع أن يقدم شهادة التصديق الإلكتروني الخاصة بالتوقيع الإلكتروني والتي تثبت نسبة التوقيع

=وفي الحالة العكسية، يؤشر القاضي على الوثيقة محل النزاع، ويأمر بإيداع أصلها بأمانة الضبط، كما يأمر بإجراء مضاهاة الخطوط، اعتمادا على المستندات أو على شهادة الشهود، وعند الاقتضاء، بواسطة خبير.

يبلغ ملف القضية إلى النيابة العامة لتقديم طلباتها المكتوبة.

وإذا عرضت القضية أمام القاضي الجزائي، يتم إرجاء الفصل في دعوى مضاهاة الخطوط إلى حين الفصل في الدعوى الجزائية».

(1)- أكد على هذا المبدأ القرار الصادر عن المحكمة العليا بتاريخ (28 ماي 1990) ملف رقم **(53931)** والذي جاء فيه ما يلي: «من المقرر قانونا أن العقد العرفي يعتبر صادرا ممن وقعه ما لم ينكره صراحة. أما ورثته أو خلفه فلا يطلب منهم ذلك ويكفي أن يحلفوا يمينا بأنهم لا يعلمون أن الخط أو الإمضاء هو لمن تلقوا منه هذا الحق. ومن ثم فإن القضاء بما يخالف هذا المبدأ يعد خطأ في تطبيق القانون». قرار منشور بالمجلة القضائية للمحكمة العليا، العدد الأول لسنة 1992، ص99.

(2)- من خلال إجراءات دعوى مضاهاة الخطوط، أو عن طريق شهود، أو مراجعة مستندات، أو عن طريق خبره، وفقا للإجراءات المقررة في المادة 165 وما يليها من قانون الإجراءات المدنية والإدارية.

لصاحبه، كما يجب على المحكمة أن تستعين بالخبراء لفحص المحرر الإلكتروني باستخدام وسائل تقنية تتماشى وطبيعته الإلكترونية [1].

أما إذا أقر الشخص بأن التوقيع الإلكتروني راجع إليه ولكنه ينكر صدوره منه شخصيـــا، نتيجة لفقدانه أو قرصنته نظرا لمخاطر البيئة الإلكترونية، ففي هذه الحالة يبقى المحرر الإلكتروني حجة عليه إلى أن يقيم الدليل على ما يدعيه، ولا يتم ذلك إلا عن طريق الطعن بالتزوير [2].

ذلك ما تأكده المادة (1/8/أ) من قانون اليونسترال النموذجي بشأن التوقيعـات الإلكترونية، إذ تنص على أنه: «**حيثما يمكن استخدام بيانات إنشاء التوقيع لإنشاء توقيع ذي مفعول قانوني، يتعين على كل موّقع:**

أ- أن يولي قدرا معقولا من العناية لاجتناب استخدام بيانات إنشاء توقيعه استخداما غير مأذون به...».

2- حجية المحرر العرفي الإلكتروني من حيث قوة البيانات المدونة فيه

إذا ثبـت صـــدور المحـــرر العرفي التقليدي أو الإلكتروني من الشخص المنسوب إليه، أصبح حجة من حيث صحة الوقائع الواردة فيه على الكافة بمن فيهم ذوي الشأن وكذلك على الغير، فيما عدا التاريخ فهو لا يكون حجة على الغير إلا إذا كان ثابتا [3].

يكون المحرر العرفي كالمحرر الرسمي فيما يتعلق بسلامته المادية، فإذا ما ادعى أحد أطرافه حصول تغيير مادي في مضمونه (بياناته) بإدخال بعض البيانات أو المعلومات، أو حذف أو شطب للبيانات وذلك عن طريق استغلال التقنيات الحديثة؛ فعليه في هذه الحالة أن يطعن بالتزوير لإثبات ما يدعيه.

---

(1)- بلقاسم حامدي، إبرام العقد الإلكتروني، أطروحة مقدمة لنيل شهادة دكتوراه العلوم في العلوم القانونية، تخصص قانون أعمال، جامعة الحاج لخضر باتنة، كلية الحقوق والعلوم السياسية، 2014-2015، ص 201.

(2)- محمد حسين منصور، الإثبات التقليدي والإلكتروني، دار الفكر الجامعي، الإسكندرية، 2006، ص 91.

(3)- يعتبر من الغير بالنسبة لصحة البيانات كل من الخلف العام والخلف الخاص والدائنين، على عكس الغير الذين سيتم ذكرهم بالنسبة لثبوت التاريخ. **أحمد عبد الرزاق السنهوري**، مرجع سابق، ص 202.

3- حجية تاريخ المحرر العرفي الإلكتروني:

تنص المادة (328) من القانون المدني الجزائري على: «**لا يكون العقد العرفي حجة على الغير في تاريخه إلا منذ أن يكون له تاريخ ثابت، ويكون تاريخ العقد ثابتا ابتداء:**

- **من يوم تسجيله؛**
- **من يوم ثبوت مضمونه في عقد آخر حرره موظف عام؛**
- **من يوم التأشير عليه على يد ضابط عام مختص؛**
- **من يوم وفاة أحد الذين لهم على العقد خط أو إمضاء.**

غير أنه يجوز للقاضي تبعا للظروف، رفض تطبيق هذه الأحكام فيما يتعلق بالمخالصة».

نستخلص من نص هذه المادة، أن المشرع الجزائري ميّز بين حجية المحرر العرفي التقليدي والإلكتروني بالنسبة للأطراف المتعاقدة، وحجيتها بالنسبة للغير؛ إذ اعتبر تاريخ المحرر بالنسبة لأطرافه جزءا من البيانات الأخرى وله نفس حجيتها، أما بالنسبة للغير فلا يعتبر المحرر العرفي ذو حجية إلا إذا كان ثابت التاريخ [1].

يعتبر من الغير في خصوص ثبوت التاريخ كل من الخلف الخاص، الدائنون الذين تعّلق حقهم بمال من أموال المدين؛ كالدائن الحاجز، والدائن الذي يتدخل في إجراءات التنفيذ، ودائنو المفلس أو المعسر، والدائنون المرتهنون وغيرهم من ذوي الحقوق المقيدة الأخرى على عقار المدين، من وقت تسجيل تنبيه نزع الملكية، والدائن الذي يرفع على مدينه دعوى عدم نفاذ التصرفات، ومن عدا هؤلاء الأشخاص، لا يعتبروا غيرا، لأنهم يعتبرون في الواقع ممثلين في التصرف موضوع المحرر، وبالتالي يمكن الاحتجاج عليهم بتاريخ المحرر العرفي، كالأصيل، والخلف العام، والدائنين العاديين[2].

---

(1)- محمد صبري السعدي، مرجع سابق، ص 74.

ومن تطبيقات المحكمة العليا في هذا الشأن المبدأ المكرس في قرار الغرفة العقارية بالمحكمة العليا الصادر بتاريخ (20 ماي 2009) ملف رقم (483177) الذي جاء فيه أن العقد العرفي حجة بين طرفيه من حيث موضوعه وتاريخه ولا يحتج به على الغير إلا إذا كان ثابت التاريخ. قرار منشور بالمجلة القضائية للمحكمة العليا، العدد 01 لسنة 2009، ص 154.

(2)- تامر محمد سليمان الدمياطي، مرجع سابق، ص 766.

والحكمة من هذه القاعدة هي منع تواطأ أطراف المحرر العرفي على الإضرار بالغير من خلال تقديم أو تأخير تاريخ المحرر، كأن يتعمد الأطراف تقديم أو تأخير المحرر العرفي قصد إخفاء أن أحدهما كان في مرض الموت، أو كان قاصرا وقت إبرام التصرف القانوني لتفادي الطعن فيه بسبب نقص الأهلية وما إلى ذلك [1].

إلا أن هذه القواعد العامة لثبوت التاريخ لا تتماشى والطبيعة التقنية للمحررات العرفية الإلكترونية؛ ما عدا في حالتي إثبات مضمون المحرر الإلكتروني في محرر آخر حرره موظف عام، أو حالة وفاة أحد الذين لهم توقيع على المحرر الإلكتروني، كما أضاف المشرع المصري شرطا أخرا وهو من يوم أن يصبح مستحيلا على أحد من هؤلاء أن يكتب أو يبصم لعلة في جسمه [2].

ونظرا لعدم إمكانية تطبيق القواعد العامة لإثبات تاريخ المحرر العرفي على المحررات الإلكترونية، حاولت بعض التشريعات استحداث طرق جديدة لإثبات تاريخ المحرر العرفي الإلكتروني، مثل ما نص عليه المشرع المصري من خلال المادة (8) من اللائحة التنفيذية لقانون التوقيع الإلكتروني [3]، حيث اشترط وجوب توافر الضوابط الفنية والتقنية التي تتيح تحديد تاريخ إنشاء الكتابة والمحرر الإلكتروني، ويتم ذلك عن طريق نظام الحفظ الإلكترونـــــي، إذ يتولى مقدم خدمات التصديق الإلكتروني تقديم خدمة البصمة الزمنية للمحرر الإلكتروني؛ والتي تربط التاريخ بالمحرر الإلكتروني بطريقة تمنع إمكانية تغيير البيانات دون اكتشافها واستنادها إلى مصدر زمني دقيق مُعتمد من سلطة التصديق الإلكتروني.

---

(1)- **أحمد عبد الرزاق السنهوري**، مرجع سابق، ص 198؛ **محمد حزيط**، مرجع سابق، ص100؛ **محمد صبري السعدي**، مرجع سابق، ص 75.

(2)- المادة 15 فقرة 2 من قانون الاثبات المصري.

(3)- تنص المادة 8 من اللائحة التنفيذية لقانون التوقيع الإلكتروني على: «**مع عدم الإخلال بالشروط المنصوص عليها في القانون، تتحقق حجية الإثبات المقررة للكتابة الإلكترونية والمحررات الإلكترونية الرسمية والعرفية لمنشئها، إذا توافرت الضوابط الفنية والتقنية الآتية:**

أ- أن يكون متاحا فنيا تحديد وقت وتاريخ إنشاء الكتابة الإلكترونية أو المحررات الإلكترونية الرسمية أو العرفية...

ج- في حالة إنشاء وصدور الكتابة الإلكترونية أو المحررات الإلكترونية الرسمية أو العرفية بدون تدخل بشري، جزئي أو كلي، فإن حجيتها تكون متحققة متى أمكن التحقق من وقت وتاريخ إنشائها ومن عدم العبث بهذه الكتابة أو تلك المحررات».

وعليه؛ فقد أوجد المشرع المصري قواعد مغايرة لثبوت تواريخ المحررات العرفية الإلكترونية تتفق وطبيعتها التقنية، ليتحرر بذلك من التبعية للقواعد العامة للإثبات، وهذا ما نأمل أن يقوم به المشرع الجزائري.

بناء على ما تقدم؛ إذا لم يحكم القاضي بإسقاط حجية المحرر العرفي الإلكتروني المُعد للإثبات، أو إنقاص حجيته بسبب عيب مادي مؤثر (مع مراعاة صعوبة ظهور ذلك في المحررات الإلكترونية نظرا لطبيعتها)، وإذا لم يحكم برد أو بطلان هذا المحرر لوجود تزوير ظاهر فيه، وإذا لم توقف حجية المحرر حتى تفصل المحكمة في صحته، فإن هذا المحرر العرفي الإلكتروني له نفس حجية المحرر العرفي التقليدي من حيث صدوره ممن وقعه وسلامته المادية، ومن حيث صحة البيانات الواردة فيه.

ثانيا: عدم المساواة بين المحرر العرفي الإلكتروني والمحرر العرفي الورقي

يوجد فرق واضح بين المحررات العرفية الإلكترونية والمحررات العرفية التقليدية من ناحية الضمانات التي يتمتع بها كل منهما، فنتيجة للطبيعة التقنية للمحرر العرفي الإلكتروني التي تمنحه مزيدا من الثقة مقارنة بالمحرر العرفي التقليدي، فالتوقيع الإلكتروني والذي يعتبر من أهم شروط صحة المحررات الإلكترونية تختلف حجيته وتتفاوت مما ينسحب ذلك على المحرر الإلكتروني، وهذا ما ينجر عنه أن افتراض موثوقية صحة التوقيع الإلكتروني المؤمن يرتفع بالمحرر الإلكتروني الممهور به إلى حد افتراض موثوقيته.

يرى بعض الفقه [1] عدم ملائمة المساواة بين المحرر العرفي الإلكتروني والمحرر العرفي التقليدي، كون هذا الأخير لا يتضمن على نفس القدر من الضمانات التي تتوافر في المحرر الإلكتروني الممهور بتوقيع إلكتروني مؤمن –والمستوفي لجميع الشروط والمتطلبات الفنية والتقنية المطلوبة قانونا–، ومن ثم افتراض صحة المحرر الإلكتروني المقترن بهذا التوقيع.

---

(1)– محمد محمد أبو زيد، تحديث قانون الإثبات "مكانة المحررات الإلكترونية بين الأدلة الكتابية"، دار النهضة العربية، 2002، ص 240 مشار إليه لدى **تامر محمد سليمان الدمياطي**، مرجع سابق، ص 778.

يترتب على نشوء هذه القرينة نتيجتان؛ تتمثل الأولى في سلامة المحرر الإلكتروني الممهور بتوقيع إلكتروني؛ مما يستلزم معه عدم حدوث أي تعديل او تلاعب في بياناته منذ تاريخ التوقيع عليه. في حين تتمثل النتيجة الثانية، في كون التوقيع الإلكتروني الممهور بالمحرر هو توقيع الشخص المنسوب إليه، وبناء عليه رضاءه وموافقته على مضمون المحرر، ومن ثم يترتب عليه أثره القانوني ويصلح للاحتجاج عليه به[1].

وعليه فالمحرر العرفي الإلكتروني الموقع توقيعا إلكترونيا مؤمنا يتمتع بقرينة موثوقية تمنحه مستوى أعلى من الأمان مقارنة بالمحرر العرفي الورقي، مما يؤدي إلى تمتع المحرر العرفي الإلكتروني بحجية تفوق المحرر العرفي التقليدي.

هذا الرأي يتوافق مع ما نص عليه القانون الفرنسي من خلال المادة (1367) [2] من القانون المدني الفرنسي، وكذا قوانين اليونسترال النموذجية سواء من خلال المادة (13)[3] من قانون اليونسترال لعام (1996) المتعلق بالتجارة الإلكترونية، أو المادة (6)[4]من قانون

---

(1)- باهة فاطمة، مرجع سابق، ص 86.

)-2(Article 1367: «**La signature nécessaire à la perfection d'un acte juridique identifie son auteur. Elle manifeste son consentement aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte. Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat** » Modifié par Ordonnance n°2016-131 du 10 février 2016 - art. 4.

(3)- تنص المادة (13) من قانون اليونسترال النموذجي بشأن التجارة الإلكترونية لسنة (1996) على: «**تعتبر رسالة البيانات صادرة عن المنشئ إذا كان المنشئ هو الذي أرسلها بنفسه ...**».

(4)- تنص المادة (6) من قانون اليونسترال النموذجي بشأن التوقيعات الإلكترونية لسنة (2001) على: «**حيثما يشترط القانون وجود توقيع من شخص، يُعد ذلك الاشتراط مستوفى بالنسبة إلى رسالة البيانات إذا استُخدم توقيع الكتروني يعوّل عليه بالقدر المناسب للغرض الذيُ أنشئت أو أبلغت من أجله رسالة البيانات، في ضوء كل الظروف، بما في ذلك أي اتفاق ذي صلة.**

تُطبق الفقرة 1 سواء أكان الاشتراط المشار إليه فيها في شكل التزام أم كان القانون يكتفي بالنص على تبعات تترتّب على عدم وجود توقيع.

يعتبر التوقيع الالكتروني قابلا للتعويل عليه لغرض الوفاء بالاشتراط المشار إليه في الفقرة 1 إذا:

(أ) كانت بيانات إنشاء التوقيع مرتبطة، في السياق الذي تُستخدم فيه، بالموقِّع دون أي شخص آخر؛

(ب) كانت بيانات إنشاء التوقيع خاضعة، وقت التوقيع، لسيطرة الموقِّع دون أي شخص آخر؛

(ج) كان أي تغيير في التوقيع الالكتروني، يُجرى بعد حدوث التوقيع، قابلا للاكتشاف؛ =

اليونسترال لعام (2001) المتعلق بالتوقيعات الإلكترونية. إذ افترض القانونين أن المحرر والتوقيع الإلكترونيين قد صدرا من مُنشؤهما دون الحاجة إلى الإقرار بهما، مع افتراض صحتهما وسلامتهما من أي تعديل أو تحريف.

ويترتب على ذلك أن من ينكر نسبة التوقيع إليه أو عدم صحته أن يثبت ذلك، فلا ينتقل عبء الإثبات للطرف الآخر كما هو الحال عليه بالنسبة للمحررات العرفية التقليدية.

وبالرجوع للقانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين، نجد أن المشرع الجزائري قد نظم الشروط والمتطلبات الفنية والتقنية لإنشاء التوقيع الإلكتروني الموصوف والتحقق منه من خلال المواد (6-7-10-11-12-13-14)، إلا أنه لم ينص صراحة من خلال هذا القانون أو غيره على قرينة افتراض صحة التوقيع الإلكتروني الموصوف، مما يحيلنا إلى تطبيق القواعد العامة في الإثبات. وعليه لا يتمتع المحرر العرفي الإلكتروني بالحجية في الإثبات، إلا إذا اعترف به من نُسب إليه أو لم ينكره صراحة، ويقع عبء إثبات صحته على من يتمسك به.

نصل أن قرينة صحة التوقيع الإلكتروني لم تأثر على عدم المساواة في الحجية بين المحررات العرفية الإلكترونية والمحررات العرفية التقليدية، فلم تنص التشريعات السالفة الذكر إلى أي مبدأ للتدرج بين المحررات، كل ما هنالك أن هذه القرينة نقلت عبء إثبات موثوقية التوقيع الإلكتروني المؤمن على من يدعي عدم صحته أو صدوره منه.

الفرع الثاني

حجية المحررات العرفية الإلكترونية غير المُعدّة للإثبات

أشرنا فيما سبق أن المحررات العرفية الإلكترونية المعدة للإثبات لا تكون دليلا كاملا إلا إذا كانت موقعة توقيعا إلكترونيا؛ باعتبار أن التوقيع هو الذي يضفي عليها الحجية القانونيـــة، غير أن هناك أنواعا أخرى من المحررات الإلكترونية لا تحمل توقيعا إلكترونيا، حيث لا

=(د) كان الغرض من اشتراط التوقيع قانونا هو تأكيد سلامة المعلومات التي يتعلق بها التوقيع وكان أي تغيير يجرى في تلك المعلومات بعد وقت التوقيع قابلا للاكتشاف...».

يكون في قصد محرريها منذ البداية اعتبارها كأدلة إثبات؛ مثل رسائل الفاكس والتلكس، رسائل البريد الإلكتروني، وكذلك الدفاتر التجارية الإلكترونية. فهل لهذه المحررات حجية في الإثبات على الرغم من أنها لم تنشأ لهذا الغرض؟، سنحاول من خلال النقاط الآتية تبيان حجية رسائل الفاكس والتلكس **(أولا)**، حجية رسائل البريد الإلكتروني **(ثانيا)**، ثم حجية الدفاتر التجارية الإلكترونية **(ثالثا)**.

أولا: حجية رسائل الفاكس والتلكس

بالرغم من الانتشار الواسع لرسائل الفاكس والتلكس خصوصا في مجال التجارة الإلكترونية، واعتبارها من صور المحررات الإلكترونية، إلا أن حجيتها أثارت جدلا فقهيا بين مؤيد ومعارض، إذ ظهرت ثلاث اتجاهات في خصوص حجيتها.

يرى الاتجاه الأول عدم تمتع رسائل الفاكس بحجية في الإثبات كونها لا تمكّن من التعرّف على هوية المرسل أو المرسل إليه، كما أنها عرضة للتزوير والتحريف في محتوياتها[1].

في حين يميز الفريق الثاني بين رسائل الفاكس والتلكس، إذ يعتبرون رسائل الفاكس مجرد قرينة للاستئناس خاضعة لسلطة القاضي التقديرية، بينما يرون أن لرسائل التلكس حجية كاملة في الإثبات لوجود جهة محايدة تعمل كوسيط ضامن لصحتها[2].

أما الاتجاه الثالث، يرى بتمتع كل من رسائل الفاكس والتلكس بحجية كاملة في الإثبات طالما لم يشترط القانون شكلا خاصا في التصرف المراد إبرامه خصوصا في المواد التجارية[3].

---

(1)- مشار لهذه الآراء لدى: **المعتصم بالله فوزي أدهم**، إثبات التعاقد الإلكتروني – دراسة مقارنة-، ط1، منشورات الحلبي الحقوقية، لبنان، 2017، ص210؛ **ناصر حمودي**، مرجع سابق، ص314؛ **يوسف أحمد النوافلة**، الإثبات الإلكتروني في المواد المدنية والمصرفية، مرجع سابق، ص 277.

(2)- **علاء محمد نصيرات**، مرجع سابق، ص53؛ **ناصر حمودي**، مرجع سابق، ص 314.

(3)- **يوسف احمد النوافلة**، الإثبات الإلكتروني في المواد المدنية والمصرفية، مرجع سابق، ص 276؛ **ناصر حمودي**، مرجع سابق، ص 315.

أما بالنسبة للتشريعات، فقد أشار القانون النموذجي بشأن التجارة الإلكترونية لعام (1996) إلى الفاكس من خلال المادة (2/أ) منه: «**يراد بمصطلح رسالة البيانات المعلومات التي يتم إنشاؤها أو إرسالها او استلامها أو تخزينها بوسائل إلكترونية أو ضوئية أو بوسائل مشابهة، بما في ذلك على سبيل الحصر تبادل البيانات الإلكترونية، أو البريد الإلكتروني، أو البرق، او التلكس، أو النسخ البرقي...**».

في حين نجد المشرع الأردني قد اعترف صراحة بالحجية القانونية لرسائل الفاكس والتلكس من خلال المادة (3/13) من قانون البيانات الأردني، حيث نصت على أن: «**...تكون لرسائل الفاكس والتلكس والبريد الإلكتروني قوة الإسناد العادية في الإثبات ما لم يثبت من نسب إليه إرسالها أنه لم يقم بذلك أو لم يكلف أحدا بإرسالها، وتكون رسائل التلكس بالرقم السري المتفق عليه بين المرسل والمرسل إليه حجة على كل منهما...**».

نلاحظ من خلال هذه المادة، أن المشرع الأردني منح المحررات الناتجة عن وسائل الاتصال الحديثة حجية المحررات العرفية، ما لم ينكر من نُسبت إليه أو نُسب إليه إرسالها ذلك. وعليه فقد ساوى المشرع الأردني بين المحررات الإلكترونية الناتجة عن وسائل الاتصال الحديثة كالفاكس والتلكس والمحررات العرفية التقليدية.

اعترف المشرع المصري في قانونه التجاري بكل من رسائل الفاكس والتلكس على أساس مبدأ حرية الإثبات في المواد التجارية، إذ تنص المادة (58) من القانون التجاري المصري رقم (17 لسنة 1999) على أنه: «**يكون إعذار المدين أو إخطاره في المواد التجارية بإنذار رسمي أو بكتاب مسجل مصحوب بعلم الوصول، ويجوز في أحوال الاستعجال أن يكون الإعذار أو الإخطار ببرقية أو تلكس أو فاكس أو غير ذلك من وسائل الاتصال السريعة**».

أما عن المشرع الجزائري، فيمكن القول أنه اعترف بها ضمنيا أو بشكل عام من خلال المادة (329) من القانون المدني التي تنص على أنه: «**تكون للرسائل الموقع عليها قيمة الأوراق العرفية من حيث الاثبات.**

وتكون للبرقيات هذه القيمة أيضا إذا كان أصلها المودع في مكتب التصدير موقعا عليه من مرسلها، وتعتبر البرقية مطابقة لأصلها حتى يقوم الدليل على عكس ذلك.

وإذا تلف أصل البرقية فلا تعتبر نسختها إلا لمجرد الاستئناس».

وعليه؛ منح المشرع الجزائري المحررات الناشئة عن الفاكس والتلكس والمعبر عنهما بالبرقية ذات القيمة الممنوحة للمحررات العرفية، شرط أن تكون موقعة من مرسلها، مع ضرورة وجود الرسالة لدى مكتب التصدير، لتفقد حجيتها في حال المنازعة في صحتها أو في حال تلف أصل البرقية.

وبالرجوع للأمر رقم (75-59) [1] المتضمن لأحكام القانون التجاري، نجده قد نص من خلال المادتين (414 و502) [2] على إمكانية استعمال أي وسيلة تبادل إلكترونية يحددها التشريع والتنظيم بمناسبة تقديم السفتجة والشيك، وهذا ما يفيد بإمكانية تقديمهما عن طريق الفاكس والتلكس.

---

(1)- أمر رقم 75- 59 مؤرخ في 29 جوان 1975، يتضمن التقنين التجاري، معدل ومتمم بموجب القانون رقم 05 -02، مؤرخ في 06 فيفري 2005، ج ر عدد 11 صادر بتاريخ 09 فيفري 2005.

(2)- تنص المادة (414) من القانون التجاري على: «يجب على حامل السفتجة الواجبة في يوم محدد أو في أجل ما من تاريخ معين أو بعد الاطلاع، أن يقدم السفتجة للدفع إما في يوم وجوب دفعها أو في أحد يومي العمل المواليين له.

ويعتبر التقديم المادي للسفتجة لغرفة المقاصة بمثابة تقديم للوفاء.

يمكن أن يتم هذا التقديم أيضا بأية وسيلة تبادل إلكترونية محددة في التشريع والتنظيم المعمول بهما».

وتنص المادة (502) من القانون ذاته على: «**يعد التقديم المادي للشيك إلى إحدى غرف المقاصة بمثابة تقديم للوفاء. يمكن أن يتم هذا التقديم أيضا، بأية وسيلة تبادل إلكترونية محددة في التشريع والتنظيم المعمول بهما**»، لقد عدلت هاتين المادتين بموجب القانون 05-02 المعدل لأحكام القانون التجاري لتضاف لهما إمكانية تقديمهما عن طريق وسائل تبادل إلكترونية محددة في التشريع والتنظيم المعمول بهما. وعليه نتساءل عما إن كان المشرع الجزائري قد اعترف صراحة بالفاكس والتلكس في التشريع والتنظيم المعمول به؟ وفي ظل غياب اعتراف صريح منه يمكن للقاضي أن يرفضهما كحجة في الإثبات على اعتبار أنهما غير محددين صراحة ضمن الأدلة الكتابية، وتجنبا لكل هذا وجب على المشرع الجزائري الاعتراف صراحة بحجية الفاكس والتلكس مثلما فعل المشرع الأردني والمصري.

ثانيا: حجية رسائل البريد الإلكتروني

سبق وأن توصلنا أن البريد الإلكتروني يُعد من أهم تطبيقات الانترنت والأكثر استخداما نظرا لسرعته الفائقة وسهولة التعامل به، كما بينا أن رسائل البريد الإلكتروني تنقسم لثلاثة أنـواع، رسائل غير موقعة ورسائل موقعة وأخرى موصى عليها.

وترتيبا على ما تقدم، سنحدد القيمة القانونية لرسائل البريد الإلكتروني ومدى حجيتها في الإثبات على النحو الآتي:

1- حجية رسائل البريد الإلكتروني غير الموقعة:

تُعد رسائل البريد الإلكتروني غير الموقعة الأكثر استخداما في الحياة اليومية، وتختلف حجيتها بحسب نوع المعاملة وكذا صفة أطرافها. فإذا كنا بخصوص معاملة تجارية بحتة (تاجر لتاجر) فإنها تخضع لمبدأ حرية الإثبات حتى ولو زادت قيمة التصرف عن النصاب المحدد قانونا، لذا يمكن الأخذ برسائل البريد الإلكتروني غير الموقعة كدليل إثبات في المواد التجـــارية، لأن الأمر يخضع في جميع الأحوال للسلطة التقديرية للقاضي [1].

أما في المواد المختلطة، وهي التصرفات التي يكون أحد طرفيها تاجرا يتعامل لصالح تجارته، في حين أن الطرف الآخر عبارة عن مستهلك، فيستفيد من حرية الإثبات غير التاجر أي المستهلك في حين يلتزم التاجر باتباع قواعد الإثبات المدنية ما لم يوجد اتفاق يقضي بغير ذلك [2].

أما في المواد المدنية، فقد اشترطت معظم التشريعات وجوب الإثبات بالكتابة إذا ما فاقت قيمة التصرف نصابا معينا، وعليه لا يجوز الاحتجاج برسائل البريد الإلكتروني غير الموقعة في هذه الحالة.

---

(1)- يوسف أحمد النوافلة، الإثبات الإلكتروني في المواد المدنية والمصرفية، مرجع سابق، ص279؛ **باهة فاطمة**، مرجع سابق، ص 108.

(2)- عائشة قصار الليل، مرجع سابق، ص 68؛ **سليماني مصطفى**، مرجع سابق، ص 189؛ **تامر محمد سليمان الدمياطي**، مرجع سابق، ص 787.

أما في حال لم تتجاوز قيمة التصرف النصاب المحدد قانونا، أو كان هناك اتفاق مسبق على الأخذ برسائل البريد الإلكتروني غير الموقع كحجية، إضافة للحالات التي توافر فيها شروط الاستثناءات المقررة على قاعدة وجوب الاثبات بالكتابة، فيجوز في هذه الحالات الأخذ برسائل البريد الإلكتروني غير الموقعة في الاثبات؛ لأنها تخضع للسلطة التقديرية للقاضي [1].

2- حجية رسائل البريد الإلكتروني الممهورة بتوقيع:

لا تختلف رسائل البريد الإلكتروني الممهورة بتوقيع إلكتروني عن المحررات العرفية الإلكترونية؛ لتوافر كل من عنصري الكتابة والتوقيع الإلكترونيين، لذا فهي تتمتع بنفس الحجية القانونية المقررة للمحررات العرفية الإلكترونية.

وبالرجوع للمادة (329 ف1) من القانون المدني الجزائري نجدها تنص على أن للرسائل الموقع عليها قيمة الأوراق العرفية من حيث الإثبات، ومادامت رسائل البريد الإلكتروني الموقع عليها تعتبر محرر إلكتروني عرفي، وبتطبيق مبدأ التعادل الوظيفي؛ فالبريد الإلكتروني الموقع يدخل ضمن الرسائل المنصوص عليها في المادة (329 ف1) أعلاه، ويترتب على ذلك اعتراف المشرع الجزائري بحجيتها في الإثبات.

3- حجية رسائل البريد الإلكتروني الموصى عليها:

على الرغم من أن التوقيع الإلكتروني يتيح تحديد هوية المتعاقدين ويضمن سلامة الرسالة، إلا أنه لا يثبت قيام المرسل بإرسال رسالة البريد الإلكتروني، ولا التاريخ الذي تم فيه هذا الإرسال. كما لا يتيح التيقّن من استلام المرسل إليه للرسالة الصادرة من المرسل[2]، هذا ما دفع إلى ظهور البريد الإلكتروني الموصى عليه.

يحقق البريد الإلكتروني الموصى عليه نفس الوظائف التي يحققها البريد التقليدي الموصى عليه، من إثبات لعملية إرسال واستلام الرسائل الإلكترونية، وإثبات هوية المرسل والمرسـل

---

(1)- **رضا محمد أزرو**، مرجع سابق، ص 153؛ **بلقاسم عبد الله**، مرجع سابق، ص 103.

(2)- **تامر محمد سليمان الدمياطي**، مرجع سابق، ص 787.

إليه، وكذا تاريخ وساعة الإرسال والاستلام. إضافة إلى هذا يتمتع بخاصية إثبات إطلاع المرسل إليه على البريد الإلكتروني وتاريخ وساعة قراءته له [1].

من أجل ذلك اعترف المشرع الفرنسي بالبريد الإلكتروني الموصى عليه من خلال المادة (8/1369) من القانون المدني الفرنسي حيث تنص على أنه: «**الرسالة الموصى عليها المتعلقة بإبرام وتنفيذ العقد يمكن إرسالها بالبريد الإلكتروني بشرط أن يكون موجها من قبل شخص ثالث من الغير وتبعا لوسيلة تتيح هويته وتحدد المرسل وتؤكد هوية المرسل إليه وتثبت فيما إذا كانت الرسالة قد استلمت من المرسل إليه أم لا**»[2]

وبذلك منح المشرع الفرنسي البريد الإلكتروني الموصى عليه الحجية نفسها للبريد التقليدي الموصى عليه، متى توافر على الشروط المنصوص عليها في المادة أعلاه، والتي تتعلق أساسا بضمان تحديد هوية أطراف المعاملة؛ المرسل والمرسل إليه، ومقدم خدمة البريد الإلكتروني الموصى عليه، مع ضمان إثبات استلام الرسالة.

أما بخصوص المشرع الجزائري، نرى أنه لا وجود لأي نص تشريعي ينظم أو يعترف بالبريد الإلكتروني الموصى عليه، هذا ما يستدعي تدخله لسد هذا الفراغ التشريعي وغيره مما تطرقنا إليه سابقا، لأن هذا العجز في تنظيم المعاملات الإلكترونية يؤدي إلى عرقلة تطبيق نظام الحكومة الإلكترونية التي تسعى الجزائر لتطبيقه.

ثالثا: حجية الدفاتر التجارية الإلكترونية

تطرقنا فيما سبق إلى مفهوم الدفاتر التجارية الإلكترونية، وذلك في معرض حديثنا عن صور المحررات الإلكترونية غير المرتبطة بشبكة الإنترنت، أما عن حجية هذه الدفاتر باعتبارها أحد أنواع المحررات العرفية الإلكترونية غير المُعدّة للإثبات، نجد أن معظم

---

(1)- باهة فاطمة، مرجع سابق، ص 111، **رضا محمد** أزرو، مرجع سابق، ص 154.

)2-(Article 1369-8: «**Une lettre recommandée relative à la conclusion ou à l'exécution d'un contrat peut être envoyée par courrier électronique à condition que ce courrier soit acheminé par un tiers selon un procédé permettant d'identifier le tiers, de désigner l'expéditeur, de garantir l'identité du destinataire et d'établir si la lettre a été remise ou non au destinataire».** Cette article Créé par Ordonnance n°2005-674 du 16 juin 2005 - art. 1 JORF 17 juin 2005.

التشريعات التي أجازت استخدام الدفاتر التجارية الإلكترونية قد منحتها حجية في الإثبات مساوية لحجية الدفاتر التجارية التقليدية، ومنها المشرع الفرنسي الذي أقر بشكل صريح بجواز إحلال الدفاتر التجارية الإلكترونية محل الدفاتر التجارية التقليدية، شرط أن تكون مطابقة ومؤرخة لحظة إنشائها بوسائل تكفل كل الضمانات في مجال الإثبات، وفقا لما ورد في المادة (R123-173) من القانون التجاري المضافة بموجب المرسوم رقم (2015-903) الصادر في (24 جويلية 2015) المتعلق بالالتزامات المحاسبية[1].

كما اعترف المشرع الأردني من خلال المادة (92) من قانون البنوك رقم (28 لسنة 2000)، إذ تنص على أنه: «... **د- تعفى البنوك التي تستخدم في تنظيم عملياتها المالية الحاسب الآلي أو غيره من أجهزة التقنية الحديثة من تنظيم دفاتر التجارة التي يقتضيها قانون التجارة النافذ المفعول، وتعتبر المعلومات المستقاة من تلك الأجهزة أو غيرها من الأساليب الحديثة بمثابة دفاتر تجارية**».

أما عن المشرع الجزائري، فنجده قد اكتفى فقط بالاعتراف بالحجية القانونية للكتابة والتوقيع الإلكترونيين في الإثبات ولم يتبع ذلك بتنظيم المستجدات التقنية الحديثة، كحال الدفاتر التجارية الإلكترونية، إذ بالعودة لنصوص القانون التجاري الجزائري لا نجد أي نص يشير إلى إمكانية استخدام الدفاتر التجارية الإلكترونية؛ وعليه فإننا نضطر في كل مرة العودة للقواعد العامة للإثبات من أجل تطبيقها على المستجدات التقنية الحديثة، والتي لا يمكن أن تتلاءم أبدا مع الطبيعة التقنية لهذه الأخيرة. الأمر الذي يستدعي من المشرع الجزائري التدخل لتنظيمها شأنه في ذلك شأن التشريعات المقارنة.

إلا أنه وعلى الرغم من عدم تنظيم المشرع الجزائري للدفاتر التجارية الإلكترونية، نرى بأن ذلك لا يحول دون استخدامها في الإثبات في حال كانت منتظمة، فالغرض الأساسي من القانون هو تيسير المعاملات الإلكترونية، ولذلك يمكن القياس على المساواة التي أطلقها

)-1(Article R123-173**: «Des documents sous forme électronique peuvent tenir lieu de livre journal et de grand-livre ; dans ce cas, ils sont identifiés et datés dès leur établissement par des moyens offrant toute garantie en matière de preuve.»** Modifié par Décret n° 2015-903 du 23 juillet 2015 relatif aux obligations comptables des commerçants, JORF n°0169 du 24 juillet 2015 page 12630 texte n° 43, art. 1.

المشرع الجزائري فيما بين المحررات التقليدية والمحررات الإلكترونية، وعليه المساواة بين الدفاتر التجارية التقليدية والدفاتر التجارية الإلكترونية في الإثبات.

نصل في الأخير إلى أن المحررات العرفية الإلكترونية تفتقد للثقة المقررة للمحررات الرسمية الإلكترونية، لذلك أقرت لها تشريعات الإثبات الإلكتروني بمرتبة أدنى من المحررات الرسمية؛ سواء من حيث ثبوت حجيتها، أو حتى في طريقة نفيها؛ فالمحررات الرسمية الإلكترونية تعتبر حجة بحد ذاتها ولا يجوز الطعن فيها إلا بالتزوير، في حين أن المحررات العرفية الإلكترونية المعدة للإثبات لا تكون حجة على الغير إلا إذا لم ينكرها صاحبها، أما المحررات العرفية الإلكترونية غير المعدة للإثبات فلا حجية لها إلا إذا أقرها القانون.

الفصل الثاني

الاعتراف التشريعي بالتوقيع الإلكتروني في الإثبات

لا تعد الكتابة وفقا للقواعد العامة دليلا كاملا إلا إذا اقترنت بتوقيع، الذي يُعد بمثابة العنصر الثاني من عناصر الدليل الكتابي المعد أصلا للإثبات، باعتباره ينسب الورقة لمن وقعها. وقد تطور التوقيع بتقدم الحضارات، حيث كانت بداياته تتم باستخدام الشمع على شكل ختم في العصور الرومانية، ليتم التوقيع في العصور الوسطى عن طريق استخدام ورق الكولان، لتستمر أساليب التوقيع في التقدم إلى غاية ظهور التوقيع اليدوي التقليدي، وبعد تطور العلم وإثباته أن كل شخص يتميز ببصمات أصابع لا يمكن أن تتشابه مع بصمات شخص آخر، تم التوصل للتوقيع عن طريق البصمة.

وقد ظلت فكرة التوقيع بمفهومها اليدوي التقليدي سائدة باعتبارها الوسيلة الوحيدة لإقرار المعلومات التي يتضمنها الدليل الكتابي، إلى غاية التغير الذي شهده العالم في الحقبة الأخيرة من القرن الماضي من ثورة في مجال تكنولوجيا المعلومات ووسائل الاتصال الرقمية، والتي انعكست نتائجها على مفهوم عناصر دليل الإثبات الكتابي، وتغيّر المفاهيم الكلاسيكية للكتابة والتوقيع وتحوّلهما من الصورة المادية المحسوسة إلى الصورة اللامادية واللامحسوسة، مما أدى إلى ظهور المحررات الإلكترونية إلى جانب المحررات التقليدية، والتوقيع الإلكتروني إلى جانب التوقيع التقليدي.

فالتوقيع إذا؛ من المبادئ الأساسية في الإثبات وشرط مهم لتوثيق أي مستند؛ سواء في المراسلات العادية أو الإلكترونية على اختلاف أنواعها ووسائطها؛ وبهذا فهو يستجيب لمتطلبات التجارة الإلكترونية؛ إذ يسهل على الأشخاص إبرام تصرفات عبر الإنترنت، وبالتوقيع تثبت الأطراف المتعاقدة موافقتها على ما هو وارد من معلومات في المستند وبالنتيجة إسناده إليها، والتوقيع في شكله الحديث يعتمد على أحدث التقنيات؛ إذ لم يعد مجرد اسم أو إشارة أو بصمة إصبع أو ختم، بل تعددت صوره؛ فمنه من يعتمد على الأرقام أو الأحرف أو الرموز، ومنه من يعتمد على الخواص الفيزيائية للإنسان، وهناك من يعتمد على

تقنية التشفير ...، هاته الصور التي تعددت وتباينت فيما بينها في قدرتها على تحقيق وظائف التوقيع، وبالتالي حجيته في الاثبات، لذا كان لزاما على مشرعي الدول التدخل لأجل التنظيم القانوني لهذا المستجد وضبط جميع جوانبه القانونية والتقنية من أجل منحه الحجية القانونية في الإثبات لضمان استقرار المعاملات التي تتم عير الوسائط الإلكترونية.

ولبيان مفهوم التوقيع الإلكتروني، وظائفه وصوره، وكذا مدى حجيته في الإثبات، وموقف التشريعات المقارنة منها، سنتطرق بالدراسة لماهية التوقيع الإلكتروني **(مبحث أول)**، لنبين فيما يلي الحجية القانونية للتوقيع الإلكتروني **(مبحث ثان)**.

المبحث الأول
ماهية التوقيع الإلكتروني

نتيجة للثورة التكنولوجية في مجال تكنولوجيا المعلومات والاتصالات ظهرت العديد من المسائل التي تحتاج إلى تنظيم، ومنها وسائل انعقاد التصرف وطرق التعبير عنه، ووسائل إثباته، والوفاء بالالتزامات الناشئة عنه. هذا بدوره أدى إلى ظهور مصطلحات جديدة كالعقود الإلكترونية، الإيجاب والقبول الإلكترونيين الكتابة والمحررات الإلكترونية، التوقيعات الإلكترونية. لذا فإن الانتقال من التوقيع التقليدي إلى التوقيع الإلكتروني لم يكن عديم الأثر، بل كان لذلك التحوّل أثرا عمليا على سمات التوقيع وخصائصه وما يقوم به من وظائف.

ونظرا للانتقال من البيئة الورقية إلى البيئة الإلكترونية، لم يعد التوقيع التقليدي بمختلف أشكاله – الإمضاء، الختم والبصمة–، الطريقة الملائمة لتوثيق المعاملات الإلكترونية، ولتعذر استخدام التوقيع التقليدي على الدعامة الإلكترونية، ظهر بديل إلكتروني يتماشى مع الطبيعة التقنية لهذه الدعامة سُمي " بالتوقيع الإلكتروني".

وعلى اعتبار أن التوقيع الإلكتروني واقعة مستحدثة، فقد سارعت العديد من المؤسسات الدولية الإقليمية والوطنية إلى تحديث المفهوم القانوني للتوقيع التقليدي، ليتلاءم مع التطور الحاصل في مجال التعاملات والتبادلات الإلكترونية، وذلك من خلال إعادة النظر فيه وتحديثه ليتماشى مع التحول في طبيعة دعامة التوقيع من المادية إلى الإلكترونية.

ولبيان مفهوم التوقيع الإلكتروني لا بد لنا من التطرق لآراء الفقهاء وما ورد بالنصوص التشريعية الدولية والوطنية المتعلقة بالإثبات الإلكتروني في معالجة أحكامه **(مطلب أول)**، وكذا التطرق بالدراسة لصوره المتعددة التي أسفر عنها التقدم التقني في مجال نظم المعلومات ووسائل إنشاء التوقيع الإلكتروني، مع بيان ما يمكنها تحقيقه من ضمان للموثوقية والأمان في المعاملات الإلكترونية، وكذا تحقيقها لوظائف التوقيع **(مطلب ثان)**.

المطلب الأول
مفهوم التوقيع الإلكتروني

لم تعد الفكرة المترسخة منذ زمن طويل والتي مفادها أن الكتابة خُلقت لكي تكون فوق دعامة مادية كالورق أو الخشب، أو الطين، مقبولة في عصر المعلوماتية الحديثة والتكنولوجيا، حيث لم تعد الدعامة الورقية الركيزة الوحيدة المستخدمة في كتابة المحررات كما رأينا في الفصل الأول من هذه الدراسة.

فنتيجة للثورة التي شهدتها المعلوماتية، أصبح من الممكن استخدام تقنية تكنولوجية لكتابة المحررات أطلق عليها اسم " الدعامة الإلكترونية"، ولتعذّر استخدام التوقيع التقليدي على هذه الركيزة بسبب طبيعتها غير المادية. أصبح من الضروري البحث عن بديل للتوقيع التقليدي يمكنه تأدية نفس الوظائف التي يقوم بها هذا الأخير، ويناسب في الوقت ذاته الركيزة الإلكترونية غير المادية، الأمر الذي أسفر عن إيجاد شكل جديد غير مـــألوف من التوقيعات، سُمي "بالتوقيع الإلكتروني" والذي يختلف عن "التوقيع التقليدي" من ناحية تكنولوجيته وشكله ومضمونه. فكانت محاولة تعريفه فقهية قضائية **(فرع أول)**، ومن بعدها قانونية **(فرع ثان)**، وهذا ما سنوضحه تباعا فيما يلي.

الفرع الأول
التعريف الفقهي والقضائي للتوقيع الإلكتروني

تقوم أشكال التوقيع الإلكتروني في مجملها على مجموعة من الرمـــوز والأرقام والبيانات، ترتكز في الأساس على معادلات لوغاريتمية، على عكس التوقيع التقليدي الذي يقوم على البساطة في إنشائه ويكون في الغالب مقصورا على التوقيع بالإمضاء، الختم، وبصمة الإصبع.

قبل أن يتم تجسيد التوقيع الإلكتروني قانونا؛ اختلف الفقه في تعريفه وإيجـاد معنـى له، بينما نجد القضاء قد عالج المسألة قبل ذلك من خلال محكمة النقض الفرنسية وهو ما سنبينه في النقطتين التاليتين:

أولا: التعريف الفقهي للتوقيع الإلكتروني

تعددّت التعاريف التي جاء بها الفقه القانوني في مجال التوقيع الإلكتروني على الرغم من اجتماعهم على ذات الفكرة [1]، حيث بنى البعض منهم تعريفه على الشكل التقني الذي هو في الأصل عبارة عن رموز أو أرقام أو حروف أو شفرات خاصة مرتبطة بالمحرر الإلكتروني، في حين أن الفريق الآخر بنى تعريفه على الجانب الوظيفي الذي يقوم به التوقيع الإلكتروني ألا وهو التعريف بهوية الموقع وإثبات رضاه على ما تم التوقيع عليه.

وفيما يلي سنستعرض أهم التعريفات التي جاء به كل اتجاه مع بيان مجموعة من الملاحظات على كل رأي، للوصول في النهاية إلى إرساء معالم مفهوم شامل للتوقيع الإلكتروني.

يرى الاتجاه الأول المبني على الجانب الوظيفي؛ ضرورة أن يقوم التوقيع الإلكتروني بنفس الوظائف التي يقوم بها التوقيع التقليدي من حيث تحديد هوية الموقّع، ورضاه بمحتوى المحرر الموقع عليه إلكترونيا، وجاءت تعريفات هذا الاتجاه للتوقيع الإلكتروني كالآتي:

حيث عرفه فريق من هذا الاتجاه بأنه: «**عبارة عن حروف أو أرقام أو رموز أو إشارات لها طابع منفرد تسمح بتحديد شخص صاحب التوقيع وتمييزه عن غيره، وهو الوسيلة الضرورية للمعاملات الإلكترونية في إبرامها وتنفيذها، والمحافظة على سرية المعلومات والرسائل**» [2].

ويرى جانب آخر من الفقه ضمن هذا الاتجاه بأنه عبارة عن: «**عناصر منفردة خاصة بالموقع، تتّخذ شكل حروف، أو رموز، أو أرقام، أو إشارات، أو غيرها توضع على محرر**

)-1(SAMBATH Hel, Le formalisme du contrat électronique dans l'ASEAN Définition et interprétation des notions d'écrit et de signature, Thèse présentée à la faculté des études supérieures en vue de l'obtention du grade de docteur en droit, faculté de droit , Université de Montréal, Mai 2013, p 20.

(2) – محمد أمين الرومي، النظام القانوني للتوقيع الإلكتروني، ط1، دار الفكر الجامعي، مصر، 2006، ص 13.

إلكتروني لتحديد شخص الموقع، وتميزه عن غيره وتعبر عن رضائه بمضمون المحرر في سرية وأمان»[1].

وعرف كذلك بأنه: «**إجراء معين يقوم به الشخص المراد توقيعه على المحرر سواء كان هذا الإجراء على شكل رقم أو إشارة إلكترونية معينة، أو شفرة خاصة، المهم في الأمر أن يحتفظ بالرقم أو الشفرة بشكل آمن وسري يمنع استعماله من قبل الغير، ويعطي الثقة في أن صدور هذا التوقيع يفيد بأنه بالفعل صدر من صاحبه، أي حامل الرقم أو الشفرة**» [2].

كما عرّفه البعض ضمن الإطار نفسه بأنه: «**مجموعة من الإجراءات التقنية التي تسمح بتحديد شخصية من تصدر عنه هذه الإجراءات وقبوله بمضمون التصرف الذي يصدر التوقيع بمناسبته**» [3].

ويرى اتجاه آخر في ذات الصياغ بأن: «**التوقيع الإلكتروني عبارة عن توقيع رقمي يرتبط بالمعلومات التي يرغب المرسل في إرسالها إلى الطرف الآخر، ويتضمن التوقيع المعطيات التي تدل على ارتباط صاحبه واعترافه بما ورد في الوثيقة الإلكترونية المرسلة**»[4].

نلاحظ من خلال التعاريف السابقة أنها ركزّت على وظيفتي التوقيع الإلكتروني، ألا وهما تحديد هوية الموقع والتعبير عن إرادته في الموافقة على مضمون المحرر الذي وقعه. في حين أنها لم تركز على صور التوقيع الإلكتروني، ولا على كيفية إنشائه، تاركة الأمر للتطور التكنولوجي حتى يتّسع مفهومها لمختلف الأشكال التي يمكن أن تظهر مستقبلا.

---

(1) – **ذنون يوسف صالح، علياء عبد الرحمان مصطفى**، التوقيع الإلكتروني وحجيته في الإثبات، مجلة جامعة تكريت للحقوق، العدد 02، الجزء الأول، العراق، 2017، ص 102، منشور على الموقع: www.iasj.net

(2) – **نجوى أبو هيبة**، التوقيع الإلكتروني، دار النهضة العربية، مصر، 2002، ص 42.

(3) – **حسن عبد الباسط جميعي**، مرجع سابق، ص 34؛ ومشار إليه كذلك لدى: **محمد بودالي**، التوقيع الإلكتروني، مجلة إدارة، العدد 26، الجزائر، 2003، ص 56.

(4) – **محمود أحمد ابراهيم الشرقاوي**، مفهوم الأعمال المصرفية الإلكترونية وأهم تطبيقاتها، بحث مقدم لمؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المنعقد ما بين (9-11) ربيع الأول الموافق 10-12 مايو 2003، كلية الشريعة والقانون وغرفة تجارة وصناعة دبي، المجلد الأول، ص 27.

بينما ركز الاتجاه الثاني على الوسيلة التي ينشأ من خلالها التوقيع الإلكتروني دون التطرق لوظائفه، ومن أبرز هذه التعاريف:

التعريف الذي يرى بأن التوقيع الإلكتروني هو: «مجموعة **من الإجراءات والوسائل التي يتبع استخدامها عن طريق الرموز أو الأرقام إخراج رسالة إلكترونية تتضمن علامة مميزة لصاحب الرسالة المنقولة إلكترونيا يجري تشفيرها باستخدام زوج من المفاتيح واحد معلن والآخر خاص بصاحب الرسالة**» [1]. نلاحظ أن هذا التعريف ركز على أحد صور التوقيع الإلكتروني، ألا وهو التوقيع الرقمي الذي يقوم على التشفير باستعمال زوج من المفاتيح (عام وخاص).

وهناك من يرى بأن: «**الإمضاءات الإلكترونية هي مجموعة من الأرقام تنجر عن حساب رياضي بعد استعمال الرقم السري**»[2].

وخر يرى بأنه: «**مجموعة الإشارات المذيّلة في نهاية السند وفق إجراءات حسابية وخوارزمية بحيث يستحيل سرقته أو الولوج إليه**»[3].

سلطت التعاريف السابقة الضوء على الجانب التقني للتوقيع الإلكتروني، إذ ركزت على الوسيلة التي ينشأ بها هذا الأخير من رموز وأرقام ومعـادلات، وأهملت الجانب الوظيفـــي لـــه، على الرغم من أن الجانبين (الوظيفي والتقني) مكملين لبعضهما البعض.

من خلال استقرائنا لهذه التعريفات نجد أن أفضل تعريف يمكن اعطاءه للتوقيع الإلكتروني، هو التعريف الذي يجمع ما بين مبدأ التناظر الوظيفي ومبدأ الحياد اتجاه

---

(1) – **شرف الدين أحمد**، التوقيع الإلكتروني وقواعد الإثبات ومقتضيات الأمان في التجارة الإلكترونية، ورقة عمل مقدمة لمؤتمر التجارة الإلكترونية المنعقد في جامعة الدول العربية، مصر، 2000، ص 03، مشار له لدى **عيسى غسان ربضي**، مرجع سابق، ص 55.

(2) – **علي كحلون**، التجارة الإلكترونية، مجلة القضاء والتشريع، العدد 02، السنة 42، تونس، فيفري 2000، ص 26.

(3) – **ضياء أمين مشيمش**، التوقيع الإلكتروني –دراسة مقارنة–، مكتبة صادر، دار المنشورات الحقوقية، لبنان، 2003، ص 124.

التكنولوجيا، والذي يمكن صياغته كالآتي: «**مجموعة من الرموز أو الأرقام أو الحروف أو الإشارات أو الأصوات، مؤلفة على شكل بيانات إلكترونية مرتبطة بمحرر إلكتروني، هدفها تمييز شخص صاحبها وتحديد هويته وتعبر دون غموض عن رضائه بما وقع عليه**».

ثانيا: التعريف القضائي للتوقيع الإلكتروني

اتبعت محكمة النقض الفرنسية في تعريفها للتوقيع الإلكتروني مسلك تعريفها للتوقيع التقليدي، فبعدما عرفت هذا الأخير على أنه: «**شهادة بخط اليد تكشف عن رضاء الموقع بهذا التصرف وتمكّن من التحقّق من إسناد التوقيع لصاحب الوثيقة**"، وقرّرت بأن:" **هذه الطريقة الحديثة (التوقيع الإلكتروني) تقدم نفس الضمانات التي يوفرها التوقيع اليدوي الذي يمكن أن يكون مقلدا، بينما الرمز السري لا يمكن أن يكون إلا لصاحب الكارت فقط**»[(1)].

حرص القضاء بعد ذلك على الاعتداد بهذا النوع الجديد من التوقيعات وبيّن بأنه يشكل توقيعا صحيحا يعتد به قانونا، وعرفّه بأنه: «**كل رمز خطي مميز وخاص يسمح بتحديد وتشخيص صاحبه بدون لبس ولا غموض وانصراف إرادته الصريحة للالتزام بمحتوى ما تم التوقيع عليه**»[(2)].

أقر هذا الاتجاه القضاء الفرنسي في حكم لمحكمة النقض الفرنسية بتاريخ (1989/11/18) بخصوص قبول التوقيع الرقمي في حالات الوفاء بالبطاقة البنكية تطبيقا لحكم محكمة النقض الفرنسية السابق المشهور بـ" كريديكاس" "crédicas"[(3)] أين أسست حكمها على قواعد الإثبات المنصوص عليها في المادتين (1134 و 1341) من التقنين المدني

---

(1)- مشار له لدى **ناصر حمودي**، مرجع سابق، ص 327.

(2) -" constitue une signature valable, toute marque distinctive et personnelle manuscrite permettant d'individualiser son auteur sans doute possible, et traduisant la volonté non équivoque de celui-ci de consentir à l'acte" Paris 22 mai 1975, désigné par **NAIMI- CHARBONNIER Marine**: La formation et l'exécution du contrat électronique, Thèse De Doctorat, Université Panthéon- Assas, Paris II , 2003, p:142.

(3)- أنظر وقائع هذه القضية لدى: **محمد السعيد رشدي**، حجية وسائل الاتصال الحديثة في الإثبات، دار النشر الذهبي، مصر، د ت ن، ص 53؛ مشار إليه لدى **ناصر حمودي**، مرجع سابق، ص 328.

الفرنسي اللتان تجيزان للأفراد مخالفة أحكامهما باعتبارهما قاعدتين مكملتين غير آمرتين، كما قررت ذات المحكمة في تقريرها السنوي لعام (1989) أن :" **التوقيع الذي يتم بتلك الإجراءات الحديثة (التوقيع المعلوماتي) يقدم الأمان والضمان والثقة التي يقدمها التوقيع الخطي، بل قد يفوقه بكثير، حيث أن الرقم السري للبطاقة البنكية لا يعرفه إلا صاحبها**". وهو الاتجاه الذي جاء من قبل محكمة استئناف مونبلييه في (09-04-1987) حيث اعترفت بالتوقيع الإلكتروني وجاء في حيثيات الحكم ما يلي:" **إنه طالما صاحب البطاقة هو الذي قام باستخدامها، وهو الذي قام أيضا بإدخال الرقم السري في نفس الوقت، فإنه يكون قد عبر عن رضاه وقبوله سحب هذا الرقم المسجل، وبناء عليه فإن شركة كريديكاس قد قدمت دليلا كافيا على ديونها بواسطة تسجيل الآلة لتلك العملية والتي كان يتعذّر قبولها لو لم يكن استخدام البطاقة متزامنا مع إدخال الرقم السري**".

غير أنه ولأجل تحقيق الدقة والفعالية والأمن المطلوبين في نظام المعلوماتية، وقصد إضفاء مصداقية عليها، قضت محكمة النقض الفرنسية في حكمها بتاريخ (1996/11/26) بشأن صحة المبادلات المالية، أنه بناء على نص المادة (130) من التقنين التجاري الفرنسي، فإن التوقيع الصادر من الشخص الذي يدعي صحته وصلاحيته لا يتم بمجرد ذكر الرقم السري في النص المرسل بواسطة التلكس، إذ أن هذا الرقم لا يعدو أن يكون المفتاح السري[1].

بعد ما بينا تعدد الآراء الفقهية والقضائية في تعريفها للتوقيع الإلكتروني، اتجهت التشريعات الحديثة لتناول المسألة على مختلف المستويات الدولية والإقليمية والوطنية، وهو الأمر الذي سنوضحه فيما يلي.

(1)- مشار إليه لدى: **ناصر حمودي**، مرجع سابق، ص 328.

الفرع الثاني

التعريف القانوني للتوقيع الإلكتروني

يضفي التوقيع الإلكتروني صفة الإلزامية للمحرر الإلكتروني، باعتباره أحد متطلبات قيام المحررات الإلكترونية؛ إذن لا قيمة لهذه الأخيرة إذا لم تكن موقعة بذات الطريقة. لذا تصدت العديد من التشريعات التي نظمت البنية القانونية للتعاملات الإلكترونية إلى مسألة تعريف التوقيع الإلكتروني، وعليه سنستعرض تعريف التوقيع الإلكتروني في قوانين بعض المنظمات واللجان الدولية، لنتبعها بتعريفه في أهم القوانين الوطنية الغربية منها والعربية.

أولا: تعريف التوقيع الإلكتروني في التشريعات الدولية

أثبت لنا الواقع العملي أن استخدام التوقيع الإلكتروني سبق بزمن طويل صدور التشريعات الدولية والوطنية التي نظمت فكرته، لذا عمدت هذه التشريعات إلى إعطاء تعريف شامل للتوقيع الإلكتروني. وأهم منظمتين قدمتا تعريف له، هما منظمة الأمم المتحدة عن طريق لجنتها للقانون التجاري الدولي "اليونسترال"، والاتحاد الأوروبي كمنظمة إقليمية.

1 – لجنة الأمم المتحدة للقانون التجاري الدولي (اليونسترال):

لم يعرف قانون اليونسترال النموذجي بشأن التجارة الإلكترونية لسنة (1996) التوقيع الإلكتروني، بل اكتفى بالإشارة إلى وظائفه من خلال نص المادة (7) على أنه: «**عندما يشترط القانون وجود توقيع من شخص يستوفي ذلك الشرط بالنسبة لرسالة البيانات إذا:**

أ)– استخدام طريقة لتعيين هوية ذلك الشخص، والتدليل على موافقة ذلك الشخص على المعلومات الواردة في رسالة البيانات.

ب)– كانت تلك الطريقة جديرة بالتعويل عليها بالقدر المناسب للغرض الذي أنشئت أو أبلغت من أجله رسالة البيانات، في ضوء كل الظروف بما في ذلك أي اتفاق متصل بالأمر»[1].

)-1(http://www.uncitral.org

وفي سنة (2001) صدر عن ذات اللجنة قانون اليونسترال النموذجي بشأن التوقيعات الإلكترونية، حيث تولى هذا القانون تعريف التوقيع الإلكتروني من خلال المادة (2/أ) منه التي اعتبرته بأنه: «بيانات **في شكل إلكتروني مدرجة في رسالة بيانات، أو مضافة إليها أو مرتبطة بها منطقيا، يجوز أن تستخدم لتعيين هوية الموقع بالنسبة إلى رسالة البيانات، ولبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات**»[1].

يظهر لنا من خلال نص المادتين (2/أ) من قانون التوقيعات الإلكترونية، والمادة (7) بشأن التجارة الإلكترونية أنهما أخذتا بالمفهوم القانوني الوظيفي للتوقيع الإلكتروني، أين تم التركيز على وظيفتي التوقيع الأساسيتين وهما تحديد شخص الموقع والتأكيد على أن إرادته اتجهت للالتزام بما وقع عليه.

نلاحظ كذلك أن نص المادة (2/أ) من قانون التوقيعات الإلكترونية، لم تحدد التقنية التي يتم بها إجراء التوقيع الإلكتروني، إذ يمكن أن يتم بأي تقنية طالما استوفت وظائف التوقيع الإلكتروني، حيث أن لجنة "اليونسترال" أرادت بذلك توسيع نطاق تطبيقه ليشمل كافة التقنيات المتوفرة، والتي يمكن أن تظهر مستقبلا.

2 – التوقيع الإلكتروني في التوجيهات الأوروبية

حدد التوجيه الأوروبي (1999/93)[2] في نصوصه مستويين للتوقيع الإلكتروني، المستوى الأول عرف من خلاله التوقيع الإلكتروني البسيط من خلال نص المادة (2/أ) منه بأنه: «**بيانات في شكل إلكتروني مضافة أو مدرجة في بيانات أخرى أو مرتبطة بها منطقيا والتي تستخدم كطريقة للتوثيق**»، أما المستوى الثاني فهو التوقيع الإلكتروني المتقدم:« **التوقيع الإلكتروني المتقدم: هو توقيع إلكتروني يستجيب للمتطلبات التالية:**

---

(1) - **http://www.uncitral.org**

(2) - Directive n° 1999/93/CE du Parlement Européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques, JO L 13 du 19.1.2000. Disponible sur le site :

http://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:31999L0093

- أن يكون مرتبط بالموقع شخصيا بشكل فريد؛

- أن يكون قادرا على تحديد هوية الموقع؛

- أن ينشأ بوسائل موضوعة تحت رقابة صاحب التوقيع؛

- مرتبط مع المعلومات المحتواة في الرسالة حي أن يكشف أي تغيير في المعلومات».

إلا أن هذا التوجيه ألغي سنة (2014) وذلك بصدور التنظيم الأوروبي رقم (2014/910) الصادر عن البرلمان الأوروبي في (23 جويلية 2014) المتعلق بتحديد الهوية الإلكترونية وخدمات الثقة في المعاملات الإلكترونية داخل السوق الداخلي[1]، أين عرف التوقيع الإلكتروني من خلال نص المادة (10/3) منه بأنه عبارة عن:« **بيانات في شكل إلكتروني مضافة أو مرتبطة منطقيا ببيانات أخرى في شكل إلكتروني، والتي يستعملها الموقع للتوقيع»**[2].

إن صياغة هذه المادة لا تختلف كثيرا عن صياغة المادة الملغاة في ظل التوجيه (1999/93)، وإنما استبدل المشرع الأوروبي عبارة " تستخدم كطريقة للتوثيق" التي كانت في ظل التوجيه القديم بعبارة " التي يستعملها الموقع للتوقيع"، وحسن ما فعل؛ ذلك أن البيانات

---

(1) - Règlement (UE) No 910/2014 du parlement Européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques dans le marché intérieur et abrogeant la directive 1999/93/CE.

يهدف هذا التنظيم أساسا إلى إزالة كل العقبات أمام السوق الأوربية الداخلية، وتدعيما للثقة في المعاملات الإلكترونية، إضافة إلى تعزيز الأمن القانوني عند استخدام وسائل تحديد الهوية الإلكترونية وخدمات التوثيق.

كما أن هذا التنظيم يعتبر أكثر إلزاما من التوجيه الأوروبي (1999/93) الملغى حيث يعتبر بمثابة قانون موحد يطبق مباشرة على الدول الأعضاء، ويحل تلقائيا محل القوانين المخالفة له.

لمزيد من التفصيل راجع في ذلك:

Didier. GOBERT, « Le règlement Européen du 23 juillet 2014Sur l'identification électronique et les services de confiance (Eidas° : analyse approfondie », juin 2015, article disponible sur : http://www.caprioli-avocats.com/images/pdf/reglement IDAS.pdf

(2) - Article 3/10 du le règlement n°910/2014 : « signature électronique », des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer ». voir sur : http://data.europa-en/eli/reg/2014/910/oj

المشكلة للتوقيع هي وسيلة للتوقيع، ولا تكون كوسيلة للتوثيق إلا إذا استوفت المتطلبات القانونية والفنية المطلوبة لضمان موثوقيتها في الإثبات[1].

أشار التنظيم الأوروبي (2014/910) إلى ثلاث أنواع من التوقيعات الإلكترونية على خلاف ما جاء به التوجيه الأوروبي الملغى (1999/93) وتتمثل هذه الأنواع في كل من التوقيع الإلكتروني البسيط في المادة (10/3) سالفة الذكر، وفي نفس المادة وفي فقرتها الموالية (11/3)[2] تطرق إلى التوقيع الإلكتروني المتقدم وعرفه بأنه: «**التوقيع الإلكتروني المتقدم هو التوقيع الذي يفي بالمتطلبات المنصوص عليها في المادة 26** »، وباستقراء نص المادة (26) من التنظيم الأوروبي (2014/910) نجدها تنص على مجموعة من الشروط، حيث عرفت التوقيع الإلكتروني المتقدم بأنه: «**التوقيع الذي يفي بالمتطلبات التالية:**

1- أن يكون مرتبط بالموقع بصفة منفردة؛

2- أن يحدد هوية الموقع؛

3- أن يتم إنشاؤه من خلال معطيات إنشاء توقيع إلكتروني تمكن الموقع من استخدامها بدرجة عالية من الأمان وتكون موضوعة تحت الرقابة الحصرية للموقع؛

4- أن يكون مضاف إلى معطيات مرتبطة بالتوقيع بحيث يمكن كشف أي تعديل عليها»[3].

أما النوع الثالث من التوقيعات فقد تم النص عليه في المادة (12/3)[4] من التنظيم الأوروبي السابق وأطلق عليه مصطلح التوقيع الإلكتروني المؤهل وهو: «**توقيع إلكتروني**

---

(1) – باهة فاطمة، المرجع السابق، ص 137،138.

(2) - Article (3/11) du règlement n° 910/2014 : **« signature électronique qui satisfait aux exigences énoncées à l'article 26 ».**

(3) - Article 26 du règlement (u e) n°910/2014 **: « une signature électronique avancée doit répondre aux exigences suivantes :**

(A)- il est uniquement lié au signataire ;

(B)- il est capable d'identifier le signataire ;

(C)- il est crée à partir de données de création de signature électronique que le signataire peut, avec un haut niveau de confiance, utiliserons son seul contrôle ; et

(D)- il est lié aux données signées avec celle-ci de telle sorte que toute modification ultérieure des données soit détectable ».

(4) - Article (3/12) du règlement (u e) n°910/2014 **« signature électronique qualifiée : une signature électronique avancée qui est criée par un dispositif de création de signature électronique qualifiée et qui est basée sur un certificat qualifié pour les signatures électroniques ».**

متقدم يتم إنشاؤه باستخدام جهاز إنشاء توقيع إلكتروني ويستند إلى شهادة مؤهلة للتوقيعات الإلكترونية».

يتضح لنا من خلال التعريفات السابقة، أن التنظيم الأوروبي عرف التوقيع الإلكتروني بناء على الوظائف التي يقوم بها التوقيع منتهجا في ذلك ما جاء به قانون اليونسترال النموذجي للتوقيعات الإلكترونية، ثم أضاف نوع جديد وهو التوقيع الإلكتروني المتقدم، أين يكون مستوى الأمان في أعلى درجاته وذلك من خلال تحقيقه لمجموعة من المتطلبات، ليضيف على هذا النوع المتقدم درجة أعلى من الموثوقية إذا استند إلى شهادة مؤهلة للتوقيعات الإلكترونية، أين يتم الاعتراف به في كل الدول الأعضاء الأخرى؛ حيث نص في المادة (3/25)[1] من التنظيم الأوروبي: « **يتم الاعتراف بالتوقيع الإلكتروني المؤهل القائم على شهادة مؤهلة صادرة في إحدى الدول الأعضاء كتوقيع إلكتروني مؤهل في جميع الدول الأعضاء الأخرى».**

ثانيا: تعريف التوقيع الإلكتروني في التشريعات الوطنية.

تطرقت العديد من التشريعات الوطنية الغربية منها والعربية إلى تعريف التوقيع الإلكتروني محاولة بذلك توضيح نظامه القانوني ولتجنب أي إلتباس قد يواجـــه هذا المفهـــوم المستحدث، ولبث الأمان والثقة في نفوس الأطراف.

تجدر الإشارة إلى أن القضاء الفرنسي سبــق المشرع في اعترافه بالتوقيـــع الإلكـــتروني، فقد أصدرت محكمة النقض الفرنسية قرارا لها جاء فيه: «**إن التوقيع الإلكتروني يتم عن طريق عدة وسائل منها التشفير والبطاقة الذكية والرمز السري والإمضاء البيومتري المتصل بجسد المتعامل كالبصمة وقزحية العين، والإمضاء الإلكتروني الديناميكي وغيرها**»[2].

---

(1) - Article (25/3) du règlement (u e) n°910/2014 : « **une signature électronique qualifiée basée sur un certificat qualifiée délivré dans un état membre est reconnue comme signature électronique qualifiée dans tous les autres états membres ».**

(2)– مشار له لدى: **المعتصم بالله فوزي أدهم**، مرجع سابق، ص 348؛ **سعدي الربيع**، حجية التوقيع الإلكتروني في التشريع الجزائري، أطروحة لنيل شهادة الدكتوراه في العلوم، كلية الحقوق والعلوم السياسية، جامعة باتنة –01–، 2016، ص 48.

أجرى المشرع الفرنسي تعديلا على القانون المدني – الجانب الخاص بالإثبات– لتكييفه مع تكنولوجيا المعلومات والتوقيع الإلكتروني وذلك وفقا للأحكام الواردة في التوجيه الأوروبي (99/93) المتعلق بالتوقيع الإلكتروني، حيث أنه من خلال القانون رقم (2000–230)، الصادر بتاريخ (13مارس 2000) ومن خلال المادة (4/1316) منه، والتي أصبحت بموجب المادة (4) من الأمر (2016 –131) المؤرخ في (10 فبراير 2016) السالف الذكر، المادة (1367) والتي تنص على أن: «**التوقيع اللازم للاعتداد بالتصرف القانوني يحدد هوية مصدره، ويعبر عن قبول الأطراف بالالتزامات المترتبة عن هذا التصرف وحينما يوضع التوقيع بواسطة موظف عام يضفي على التصرف القانوني طابع الرسمية...**» ثم جاء في فقرتها الثانية: «**...عندما يكون إلكترونيا، فإنه يتمثل في استخدام وسيلة موثوق بها لتحديد الشخص تضمن صلته بالتصرف الذي وقع عليه، وتفترض موثوقية هذه الوسيلة ما لم يوجد دليل مخالف، كلما نشأ هذا التوقيع محددا لهوية الموقع وضامنا لسلامة المحرر وذلك وفق الشروط المحددة بمرسوم صادر عن مجلس الدولة**»[1].

يتضح من هذه المادة، أن المشرع الفرنسي قد وضع مفهوما موّسعا للتوقيع ولم يفرق بين التوقيع التقليدي والتوقيع الإلكتروني، وإنما ركّز على الوظائف التي يؤديها في الإثبات، واشترط المشرع الفرنسي أن تكون وسيلة إنشاء التوقيع الإلكتروني موثوقا فيها[2].

ولتوضيح تطبيق المادة سالفة الذكر، صدر المرسوم (2017– 1416) [3] المؤرخ في (28 سبتمبر 2017) والذي ورد فيها أن موثوقية التوقيع الإلكتروني مفترضة إذا كانت الوثيقة موقعة توقيعا إلكترونيا مؤهلا أو معززا، ويكون التوقيع الإلكتروني بهذا الشكل إذا توفرت فيه

---

(1) - Article 1367 : « **La signature nécessaire à la perfection d'un acte juridique son auteur .elle manifeste son consentement aux obligations qui découlent de cet acte-quand elle est opposée par un officier public ,elle confère l'authenticité à l'acte .lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache la fiabilité de ce procédé est présumée ,jusqu'à preuve contraire, lorsque la signature électronique est criée ,l'identité de signature assurée et l'intégrité de l'acte garantie ,dans des conditions fixées par décret en conseil d'état** ».modifié par ordonnance n°2016-131 du 10 février 2016-act 4.

(2) – باهة فاطمة، مرجع سابق، ص 135.

(3) - Décret n°2017-1416 du 28 septembre 2017 relatif à la signature électronique, JORF n° 0229 du 30 septembre 2017 tete n°8.

الشروط المنصوص عليها في المادة (26) من التنظيم الأوروبي (2014/910) والتي تطرقنا إليها سالفا.

أما عن المشرع التونسي فقد كانت له الريادة مقارنة بالمشرعين العرب في تنظيم المعاملات الإلكترونية بإصداره للقانون (2000/83) الخاص بالمبادلات والتجـارة الإلكترونيـة، وعيا منه بأهمية تنظيم هذا النوع الجديد من المعاملات، وبالرجوع لنصوص القانون المذكور أعلاه نجد أن المشرع التونسي لم يقدم تعريفا للتوقيع الإلكتروني وإنما نص في الفصل الخامس منه على أنه: «**يمكن لكل من يرغب في إمضاء وثيقة إلكترونية إحداث إمضائه الإلكتروني بواسطة منظومة موثوق بها يتم ضبط مواصفاتها التقنية بقرار من الوزير المكلف بالاتصالات**».

وعرف منظومة إحداث الإمضاء في الفصل الثاني من القانون نفسه بأنها: «**مجموعة وحيدة من عناصر التشفير الشخصية أو مجموعة من المعدات المهيأة خصيصا لإحداث إمضاء إلكتروني**».

يقصد بعبارة مجموعة وحيدة أنها تخص شخصا واحدا؛ وذلك حتى يمكن التمييز والتفرقة بين التوقيع الإلكتروني لشخص وآخر [(1)].

نلاحظ أنه، على الرغم من اعتراف المشرع التونسي بالتوقيع الإلكتروني إلا أنه لم يُقم بتعريفه تعريفا مباشرا، وإنما اكتفى بالنص على منظومة إحداثه، مع تحديد الضوابط والأسس والضمانات المتعلقة بهذا التوقيع من خلال إحداث منظومة توقيع موثوق بها.

في حين عرف المشرع الأردني التوقيع الإلكتروني في القانون رقم (15 لسنة 2015) المتعلق بالمعاملات الإلكترونية من خلال مادته (2) بنصها على أن: «**التوقيع الإلكتروني: البيانات التي تتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها وتكون مدرجة بشكل**

(1) – **بلقنيشي حبيب**، إثبات التعاقد عبر الانترنت (البريد المرئي) – دراسة مقارنة –، رسالة مقدمة لنيل شهادة الدكتوراه في العلوم، كلية الحقوق، جامعة وهران، 2010/2010، ص 114.

إلكتروني أو أي وسيلة أخرى مماثلة في السجل الإلكتروني أو تكون مضافة عليه أو مرتبطة به بهدف تحديد هوية صاحب التوقيع وانفراده باستخدامه وتمييزه عن غيره».

ركزّ المشرع الأردني من خلال هذا التعريف على وظائف التوقيع من تحديد هوية الموقع والتزامه بما وقع عليه، وهو إقرار لمبدأ النظير الوظيفي، كما جاء هذا التعريف متناسقا مع مبدأ الحياد إزاء التكنولوجيا؛ إذ أنه لم يقصر التوقيع الإلكتروني على شكل معين، وإنما ترك المجال مفتوحا لما قد تنتجه التكنولوجيا مستقبلا. وبذلك انتهج المشرع الأردني في تعريفه للتوقيع الإلكتروني ما نصت عليه قواعد قانون اليونسترال.

وبالنسبة لمصر فقد وضعت قانونا خاصا بالتوقيع الإلكتروني، ألا وهو القانون (15 لسنة 2004) الخاص بتنظيم التوقيع الإلكتروني[1]، حيث عرفت في المادة (1/ج) التوقيع الإلكتروني بأنه: «**ما يوضع على محرر إلكتروني ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها ويكون له طابع متفرد يسمح بتحديد شخص الموقع ويميزه عن غيره».**

بناء على هذا التعريف، نلاحظ أن المشرع المصري مزج ما بين التعريف التقني والتعريف الوظيفي، فقد اعتبر التوقيع الإلكتروني أنه مجموعة من الحروف أو أرقام أو رموز أو إشارات والتي تشكل طرقا عدة للتوقيع الإلكتروني، ثم فتح الباب لأي تقنية قد تظهر وذلك تحت عبارة "وغيرها ".

اشترط المشرع المصري بعد ذلك أن تكون بيانات إنشاء التوقيع الإلكتروني ذات طابع منفرد، ويعتبر هذا الشرط بالغ الأهمية حتى يضمن سرية التوقيع الإلكتروني؛ وبضمان سرية التوقيع الإلكتروني يتم تحديد هوية الموقع وتمييزه عن غيره وهي الوظيفة الوحيدة التي نص عليها المشرع المصري في تعريفه للتوقيع الإلكتروني، دون تطرقه لشرط التعبير عن إرادة الموقع بالموافقة على مضمون السند، وربما قد افترض أن مجرد تحديد هوية الموقع تدل على قبوله بما وقع عليه.

(1)- القانون (15 لسنة 2004) الخاص بتنظيم التوقيع الإلكتروني المصري، مرجع سابق.

أضاف المشرع المصري من خلال المادة 18 من القانون نفسه شروطا حتى يضفي على التوقيع الإلكتروني الحجية الكاملة في الإثبات، وتتمثل هذه الشروط في:

- ارتباط التوقيع بالموقع وحده دون غيره؛
- سيطرة الموقع وحده دون غيره على الوسيط الإلكتروني؛
- إمكانية كشف أي تعديل أو تبديل في بيانات المحرر الإلكتروني أو التوقيع الإلكتروني.

أما عن المشرع المغربي فلم يقدم تعريفا واضحا للتوقيع الإلكتروني، لكنه حاول تعريفه من خلال الفقرة الثالثة من الفصل (2-417) من قانون الالتزامات والعقود بنصها على أنه: « ... **عندما يكون التوقيع إلكترونيا يتعين استعمال وسيلة تعريف موثوق بها تضمن ارتباطه بالوثيقة المتصلة به**». من خلال هذا التعريف، يتضح أن المشرع المغربي تبنّى التعريف الموسّع للتوقيع الإلكتروني، حيث نص على شرط واحد وهو أن تكون وسيلة التعريف موثوقا بها [1]، وأن تضمن ارتباطه بالوثيقة الإلكترونية المرتبط به بغض النظر عن شكل التوقيع الإلكتروني.

بالرجوع لنص الفقرة الثانية من الفصل (3-417) من القانون نفسه، نجدها تنص على أنه: «**يعتبر التوقيع الإلكتروني مؤمنا إذا تم إنشاؤه وكانت هوية الموقع مؤكدة وتمامية الوثيقة القانونية مضمونة، وفق النصوص التشريعية والتنظيمية المعمول بها في هذا المجال**»، أما عن شروط التوقيع الإلكتروني المؤمن فقد نصت عليها المادة (6) من القانون رقم (05-53) المتعلق بالتبادل الإلكتروني للمعطيات القانونية وهي:

- أن يكون خاصا بالموقع؛
- أن يتم أنشاؤه بوسائل يمكن للموقع الاحتفاظ بها تحت مراقبته الخاصة بصفة حصرية؛
- أن يضمن وجود ارتباط بالوثيقة المتصلة به بكيفية تؤدي إلى كشف أي تغير لاحق أدخل عليها؛

(1)- عبد الحكيم زروق، مرجع سابق، ص 35.

– أن يوضع التوقيع بواسطة آلية لإنشاء التوقيع الإلكتروني، تكون صلاحيتها مثبتة بشهادة للمطابقة.

تأسيسا على ما سبق، نجد أن المشرع المغربي بنى تعريفه للتوقيع الإلكتروني المؤمن على ضرورة توافر مجموعة من الشروط القانونية والتقنية التي تخوله تحقيق وظائف التوقيع العادي، والتي تتمثل أساسا في تحديد هوية موقع الوثيقة الإلكترونية، والتزامه بمضمون ما ورد فيها.

أما بالنسبة للمشرع الجزائري فإن أول اعتراف له بالتوقيع الإلكتروني كان من خلال نص المادة (2/327)[1] من القانون المدني التي نصت على أن: «**... ويعتد بالتوقيع الإلكتروني وفق الشروط المذكورة في المادة 323 مكرر 1 أعلاه**»، أما المادة (323 مكرر 1) من القانون المدني الجزائري فقد نصت على أنه: «**يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها**».

نلاحظ من خلال القراءة الأولية لهاتين المادتين، أن المادة (2/327) تحيلنا إلى المادة (323 مكرر1) من القانون المدني الجزائري والتي تنص على الشروط اللازم توفرها لصحة الكتابة الإلكترونية ومعها التوقيع الإلكتروني وتتمثل في:

– إمكانية التأكد من هوية الشخص الذي أصدرها؛
– أن تكون معدة ومحفوظة في ظروف تضمن سلامتها.

استخلاصا لما سبق، يتضح أن المشرع الجزائري تبنّى منهج النظير الوظيفي الذي أقرته لجنة "اليونسترال"، حيث أنه اعترف بالتوقيع الإلكتروني وساوى بينه وبين التوقيع التقليدي باعتباره نظيرا وظيفيا له.

(1)– التي عدلت سنة 2005 بموجب الأمر رقم 05–10 مؤرخ في 20 جوان 2005، يعدل ويتمم الأمر رقم 75–58 المؤرخ في 26 سبتمبر 1975 المتضمن القانون المدني ج.ر.ع 44، صادر في 26 جوان 2005.

بعد ذلك أصدر المشرع الجزائري المرسوم التنفيذي (07-162)[1] المعدل والمتمم للمرسوم التنفيذي (01-123) والمتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات، حيث عرف التوقيع الإلكتروني من خلال المادة (3 مكرر ف1) منه بأنه: «**التوقيع الإلكتروني هو معطى ينجم عن استخدام أسلوب عمل يستجيب للشروط المحددة في المادتين 323 مكرر 323 مكرر 1 من الأمر رقم 75-58 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975 والمذكور أعلاه**».

حدد بعد ذلك المشرع الجزائري شروط التوقيع الإلكتروني المؤمن في الفقرة الموالية مباشرة بنصها: «**التوقيع الإلكتروني المؤمن: هو توقيع إلكتروني يفي بالمتطلبات الآتية:**

- **يكون خاصا بالموقع؛**
- **يتم إنشاؤه بوسائل يمكن أن يحتفظ بها الموقع تحت مراقبته الحصرية؛**
- **يضمن مع الفعل المرتبط به، صلة بحيث يكون كل تعديل لاحق للفعل قابلا للكشف عنه**».

من خلال هذا المرسوم التنفيذي، نجد أن المشرع الجزائري قد قدم تعريفا مُبهما للتوقيع الإلكتروني، إلا أنه ميّز بين نوعين من التوقيعات الإلكترونية، التوقيع الإلكتروني البسيط والتوقيع الإلكتروني المؤمن.

تدارك المشرع الجزائري هذا التعريف المبهم للتوقيع الالكتروني بعدما أصدر القانون رقم (15-04) المتعلق بالتوقيع والتصديق الالكترونيين، أين عرف التوقيع الإلكتروني في مادته (2 ف1) بأنه: «**بيانات في شكل إلكتروني، مرفقة أو مرتبطة منطقيا ببيانات الكترونية أخرى، تستعمل كوسيلة توثيق**....»، وهو التعريف نفسه الذي جاء به التوجيه الأوروبي (1993/93) الملغى بالتنظيم الأوروبي (2014/910).

---

(1) – مرسوم تنفيذي رقم 07 – 162 مؤرخ في 13 جمادى الأولى عام 1428 الموافق 30 مايو سنة 2007، يعدل ويتمم المرسوم التنفيذي رقم 01 – 123 المؤرخ في 15 صفر عام 1422 الموافق ل 09 مايو سنة 2001 والمتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية، ج. ر. ع 37، صادر بتاريخ 07 يونيو 2007.

من خلال هذا النص، يتّضح جليا أن المشرع الجزائري اعتمد "مبدأ الحياد التقني" الذي أقرته المادة (3) من قانون اليونسترال النموذجي لسنة (2001)، تحت عنوان «المعاملة المتكافئة لتكنولوجيا التوقيع». حيث بإمكان هذا التعريف أن يستوعب كل التقنيات التي تتدخل في إنشاء التوقيع الالكتروني دون تفضيل تقنية على أخرى. ليوضح المشرع الجزائري من خلال المادة (6)[1] من القانون نفسه موقفه بانتهاجه للمنهج الوظيفي للتوقيع الالكتروني، حيث تنص هذه المادة على وظائف التوقيع الالكتروني والمتمثلة أساسا في: تحديد هوية الموقع، والتزامه بما وقع عليه.

نص المشرع الجزائري كذلك من خلال المادة (7) من القانون (15-04) على التوقيع الالكتروني الموصوف حيث وردت المادة كما يلي: «**التوقيع الإلكتروني الموصوف هو التوقيع الذي تتوافر فيه المتطلبات الآتية:**

1- أن ينشأ على أساس شهادة تصديق إلكتروني موصوفة؛
2- أن يرتبط بالموقع دون سواه؛
3- أن يمكّن من تحديد هوية الموقع؛
4- أن يكون مصمما بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الإلكتروني؛
5- أن يكون منشأ بواسطة وسائل تكون تحت التحكم الحصري للموقع؛
6- أن يكون مرتبطا بالبيانات الخاصة به، بحيث يمكن الكشف عن التغييرات اللاحقة بهذه البيانات».

يتضح لنا من خلال هذه المادة تبني المشرع الجزائري لنوعين من التوقيع الإلكتروني، توقيع إلكتروني بسيط وتوقيع إلكتروني موصوف يتمتع بدرجة أعلى من الموثوقية.

استخلاصا من كل التعريفات التي ذكرناها سابقا للتوقيع الإلكتروني نلاحظ:

---

(1) – تنص المادة (6) من القانون (15 – 04) المتعلق بالتوقيع والتصديق الإلكترونيين على أنه: «**يستعمل التوقيع الالكتروني لتوثيق هوية الموقع وإثبات قبوله مضمون الكتابة في الشكل الإلكتروني**».

– حرص كل من المؤسسات التشريعية الدولية والإقليمية والوطنية على أهمية الاعتراف بالتوقيع الالكتروني ومنحه نفس الحجية القانونية للتوقيع التقليدي في الإثبات.

– اعتماد التشريعات السابقة الذكر في تعريفها للتوقيع الالكتروني على المعيار الوظيفي، والالتزام بمبدأ الحياد التقني لتتمكن مستقبلا من استيعاب كل ما ينتجه التقدم العلمي من أنواع وصور جديدة للتوقيع الالكتروني، هاته الصور التي ستكون محل دراسة مفصلة في المطلب الموالي.

المطلب الثاني

صور ووظائف التوقيع الإلكتروني

تتعدد صور التوقيع الإلكتروني باختلاف التقنية المستخدمة في إنشاءه؛ فكل تقنية تستخدم في إنشاء التوقيع الإلكتروني يكون لها منظومة تشغيل تختلف عن الأخرى، الأمر الذي دفع تشريعات الدول للأخذ بمبدأ الحياد التقني عند تنظيمها للتوقيع الإلكتروني مما يسمح بقبول تقنيات جديدة في إنشاء التوقيع الإلكتروني قد تظهر مستقبلا.

وعلى الرغم من أن صور التوقيع الإلكتروني تتم كلها عبر الوسائط الإلكترونية إلا أنها تختلف فيما بينها وفقا للتقنية التي تم إنشاؤها بها، على اعتبار أن كل تقنية مستخدمة في إحداث التوقيع الإلكتروني لها درجة ثقة وأمان قانونيتين تختلف عن الأخرى.

وعليه فكل صورة من صور التوقيع الإلكتروني لها قدرات متفاوتة في تحقيق وظائف التوقيع الإلكتروني من تحديد لهوية الموقع، وقدرته على إثبات قبول الموقع على مضمون المحرر الإلكتروني، وكذا الحفاظ على سلامة محتوى ما تم التوقيع عليه.

لذا من خلال هذا المطلب سنتطرق لأهم الأنواع والصور المعروفة للتوقيع الإلكتروني حتى الآن، والتي توصلت إليها التكنولوجيا الحديثة **(فرع أول)**، لنبين فيما بعد مدى تحقق وظائف التوقيع الإلكتروني في صوره **(فرع ثان)**.

الفرع الأول
صور التوقيع الالكتروني

للتوقيع الإلكتروني عدة صور أو أشكال، وذلك راجع لتعدد التقنيات المستخدمة في تشغيل منظومة التوقيع الإلكتروني، التي أسفرت عنها التطورات التكنولوجية الحديثة والمختلفة، هذا من جهة، ومن جهة أخرى، لكون المسألة تقنية أكثر منها قانونية [1]. ومن بين أهم التواقيع الإلكترونية نذكر التوقيع الرقمي **(أولا)**، التوقيع البيومتري الذي يعتمد على الخواص الفيزيولوجية للإنسان **(ثانيا)**، التوقيع الكودي **(ثالثا)**، التوقيع بالقلم الالكتروني **(رابعا)**.

أولا: التوقيع الرقمي

عرّفت المنظمة العالمية لتوحيد المعايير (iso) في المعيار المتعلق بهندسة الأمان للأنظمة المفتوحة رقم(iso7489-02) لعام (1989)، التوقيع الرقمي بأنه:« **التوقيع الرقمي هو بيانات مضافة لوحدة بيانات، أو تحويل تشفيري لوحدة من البيانات يسمح للمرسل إليه بإثبات مصدر وحدة بيانات وسلامتها، ويؤمنها من التحريف أو التعديل** »[2]، وتعتبر منظمة (iso) أولى المنظمات التي اهتمت بالتوقيع الرقمي[3].

كما عرفته لجنة الأمم المتحدة للقانون التجاري الدولي في وثيقة لها مؤرخة في (31 ديسمبر 1996)[4] بأنه: «**قيمة عددية تبصم بها رسالة بيانات وتجعل من الممكن باستخدام**

---

(1) – «يذهب بعض الفقه الأمريكي إلى تقسيم صور التوقيعات الالكترونية إلى (04) مستويات، تبعا لدرجة الأمان المتاحة مع كل توقيع: ففي المستوى الأول يكون التوقيع بالنقر على لوحة المفاتيح كدليل على الموافقة، والمستوى الثاني هو الذي يستخدم فيه كلمات السر وبطاقات الائتمان، والمستوى الثالث هو الذي يعتمد على قياسات الخواص الحيوية للإنسان، والأخير هو التوقيع الرقمي المعتمد على بنية المفتاح العام».

أنظر: **محمد محمد سادات**، أثر تنوع التوقيعات الالكترونية على حجية العقود العرفية الالكترونية، مرجع سابق، ص 148.

(2) - « Signature numérique : données ajoutées à une unité de données, ou transformation cryptographique d'une unité de données permettant à un destinataire de prouver la source et l'intégrité de l'unité de donnée et protégeant contre la contrefaçon » cité par : **Thierry Piette COUDOL,** échanges électroniques certification st sécurité, édition litec,2001, p127

(3) – **Thierry COUDOL Piette**, op.cit., p127

(4) - Document n° A/CN.9/WG. IV/WP.71,31 décembre 1996, V.55 disponible sur la langue arabe sur site : https://documents-ddsny.un.org/doc/UNDOC/LTD/V96/885/25/PDF/V9688525.pdf?OpenElement

إجراء رياضي معروف يقترن بمفتاح الترميز الخاص لمنشئ الرسالة، القطع بأن هذه القيمة العددية قد تم الحصول عليها باستخدام مفتاح الترميز الخاص بمنشئ الرسالة دون سواه. والإجراءات الرياضية في إنتاج توقيعات رقمية معتمدة بموجب هذه القواعد تستند إلى ترميز مفتاح عام، وعندما تطبق تلك الإجراءات الرياضية على رسالة البيانات تحدث في الرسالة تحوّلا يمكّن الشخص الذي يمتلك الرسالة المبدئية ومفتاح الترميز العام لمنشئ الرسالة من أن يبت بدقة: (أ) – فيما إذا كان التحول قد أحدث باستخدام مفتاح الترميز الخاص الذي يناظر مفتاح الترميز الخاص للمنشئ، و (ب) – فيما إذا كانت الرسالة المبدئية قد غُيّرت بعد أن أحدث فيها التحول »[1].

يتضّح لنا من خلال هذين التعريفين أن هذا التوقيع يعتمد على نظام التشفير، إذ يرتكز على تحويل البيانات من صيغة مقروءة إلى صيغة غير مقروءة[2]، معتمدا في ذلك على تقنية التشفير التماثلي والتشفير اللاتماثلي.

وآلية عمل التوقيع الرقمي تعتمد على قيام الحاسوب بتحويل المحرر المكتوب إلى أرقام وحفظها في جهاز الحاسوب؛ مع التوقيع المكون من أرقام أيضا؛ وذلك كله وفق معادلة

---

(1) - « Une valeur numérique apposée à un message de données et qui, grâce à une procédure mathématique bien connue associée à la clé cryptographique privée de l'expéditeur, permet de déterminer que cette valeur numérique a été créer à partir de la clé cryptographique privée de l'expéditeur .Les procédures mathématiques utilisées pour créer les signatures numériques sont fondées sur le chiffrement de la clé publique appliquées à un message de données ,ces procédures mathématiques opérant une transformation du message de telle sorte qu'une personne disposant du message initial et de la clé publique de l'expéditeur peut déterminer avec exactitude :
a)-si la transformation a été opérée à l'aide de la clé privée correspondant à celle de l'expéditeur ,et
b)- si le message initial a été altéré une fois sa transformation opérée

(2) – علاء محمد نصيرات، حجية التوقيع الالكتروني في الإثبات –دراسة مقارنة–، ط1، دار الثقافة للنشر والتوزيع، الأردن، 2005، ص37؛ **كامران الصالحي**، الطبيعة القانونية لمسؤولية مزود خدمات التصديق، مؤتمر المعاملات الالكترونية (التجارة الالكترونية– الحكومة الالكترونية)، جامعة الإمارات العربية المتحدة، كلية الحقوق والشريعة، ماي2009، ص632؛ أنظر أيضا:

BENSOUSSAN Alain, Internet : aspects juridiques,2eme édition revue et augmentée, édition HERMES, Paris 1998, pp 70 et 55.

رياضية خاصة تتوفر لدى طرفي العقد، كما يمكن للطرفين إعادة المعادلة الرياضية إلى شكلها الأصلي[1]، ويتم تشفير الرسالة بطريقتين:

1- التشفير التماثلي:

يُعرف كذلك بالنظام "السيمتري" وهي طريقة تعتمد على مفتاح موحد لإغلاق بيانات المحرر وإعادة فتحها، حيث يرسل المفتاح مع الرسالة من المرسل إلى المرسل إليه مشكلا بذلك إحدى عيوب هذا النظام؛ وذلك لإمكانية قرصنة المفتاح. لذا لابد من إيجاد طريقة آمنة تضمن سلامة المفتاح أثناء تبادله[2]، أو أن يتم التعامل بهذه التقنية في الشبكات المغلقة، كشبكة الإنترانت(INTRANET) وشبكة الاكسترانت(EXTRANET)[3] .

2- التشفير اللاتماثلي:

يعرف بالتشفير "اللاتماثلي" أو التشفير "بالمفتاح غير المتماثل" أو النظام "الأسيمتري"، وهو الصورة الحديثة المتبعة في إجراء التوقيع الرقمي، إذ يقوم على مفتاحين لإجراء عملية التشفير، يسمى الأول بالمفتاح الخاص (Clé privé)، ويكون سري وخاص بصاحبه الذي يقوم بعملية التشفير، في حين يعرف الثاني بالمفتاح العام (Clé publique) بحيث يكون معروفا

---

(1) – **يوسف أحمد النوافلة**، الإثبات الالكتروني في المواد المدنية والمصرفية – دراسة مقارنة–، مرجع سابق، ص 90؛ **كرازدي سارة، لجلط فواز**، الحجية القانونية للتوقيع الإلكتروني كدليل إثبات، المجلة الجزائرية للأمن الإنساني، المجلد 06، العدد 01، جانفي 2021، ص1410.

(2) – **عيسى غسان الريضي**، مرجع سابق، ص68؛ **أزرو محمد رضا**، مرجع سابق، ص216.

(3) – شبكة **الانترانت** " **INTRANET**": هي عبارة عن سلسلة من شبكات المعلومات يمتلكها مشروع أو مؤسسة واحدة وهذه الشبكات قد تكون شبكات داخلية محدودة النطاق تتصل ببعضها البعض داخل نفس المكان أو تكون شبكات واسعة النطاق تتصل ببعضها البعض في أماكن مختلفة ومتعددة.

شبكة الاكسترانت "**EXTRANET**": هي شبكة خاصة مملوكة لمنشأة معينة تلتزم بذات البروتوكولات التي تستخدمها شبكة الإنترنت في إجراء عملية الاتصال وتبادل البيانات والمعلومات بين المنشأة وموزعيها أو مورديها أو شركائها أو حتى عملائها بصورة آمنة، إذ أن هذه البيانات تتعلق في غالب الأمر بصفقات وعقود ومعاملات تجارية وعروض وكذلك بيانات سرية تخص العملاء. نقلا عن: **لالوش راضية**، أمن التوقيع الالكتروني، مذكرة لنيل شهادة الماجستير في القانون، فرع القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2012، ص52.

للمرسل إليه حتى يتمكن من فك التشفير، وليتحقق من شخصية الموقع، ويتأكد من صحة وسلامة المحرر [1].

إن هذا التميّز بين المفتاحين لا ينفي ترابطهما في أداء عملهما، فإذا استعمل المفتاح الخاص في تشفير الرسالة، فلا يمكن فك التشفير إلا بالمفتاح العام، كما أنه لو عرف أحد المفتاحين فلا يمكن معرفة الآخر حسابيا [2].

بالرجوع للقانون (15-04) المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين سالف الذكر، نجده قد عرف كل من المفتاحين العام والخاص مطلقا عليهما تسمية مفتاح التشفير الخاص ومفتاح التشفير العمومي في نص المادة (02 ف 8 و9) معرفا لهما كالآتي:

تنص المادة (2 ف 8) على أن مفتاح التشفير الخاص: «...**هو عبارة عن سلسلة من الأعداد يحوزها حصريا الموقع فقط، وتستخدم لإنشاء التوقيع الالكتروني، ويرتبط هذا المفتاح بمفتاح تشفير عمومي**».

وتنص المادة (2 ف 9) على أن مفتاح التشفير العمومي: «...**هو عبارة عن سلسلة من الأعداد تكون موضوعة في متناول الجمهور بهدف تمكينهم من التحقق من الإمضاء الالكتروني، وتدرج في شهادة التصديق الالكتروني**».

من خلال التعريف الذي جاء به المشرع الجزائري، نجد أنه اشترط تدخل طرف ثالث موثوق يعمل على تحديد هوية صاحبه وإصدار شهادات تفيد صحته.

---

(1) - **أسامة بن غانم العبيدي**، حجية التوقيع الالكتروني في الإثبات، المجلة العربية للدراسات الأمنية والتدريب -المجلد 28- العدد 56، السعودية، ص154؛ **ثروت عبد الحميد**، التوقيع الالكتروني، ماهيته ومخاطره وكيفية مواجهتها، مدى حجيته في الإثبات، ط2، مكتبة الجلاء الجديدة، مصر، 2002، ص62؛ **كرازدي سارة، لجلط فواز**، مرجع سابق، ص 1410.

(2) - **إيمان مأمون أحمد سليمان**، الجوانب القانونية لعقد التجارة الالكترونية، رسالة دكتوراه، جامعة المنصورة، 2005-2006، ص167؛ **مصطفى هنشور وسيمة**، النظام القانوني للتوقيع الإلكتروني، مجلة الحقوق والعلوم الإنسانية، المجلد 02، العدد 24، ص 412.

نستنتج في الأخير أن التوقيع الرقمي يحقق مجموعة من المزايا؛ منها التحقّق من هوية الموقع، وصحة محتويات المعاملة الالكترونية وسريتها، وعدم إمكانية الطعن في نسبتها إلى الموقع.

ثانيا: التوقيع البيومتري

تعتبر هذه الصورة من بين أحدث صور التوقيع الالكتروني بالإضافة لكونها مكلفة، إلا أن كبريات البنوك في الدول المتقدمة تستعملها [1]. ويتميّز هذا التوقيع باعتماده على الخواص الفيزيائية لكل شخص، كبصمة الإصبع، أو بصمة العين، أو الشفاه، أو غيرها من المميزات التي يتمتع بها الشخص. وكذا دراسة المميزات التي تميزه في مظهره الخارجي، كدراسة خط الإنسان بقياس درجة ضغط اليد على القلم وكمية الاهتزازات الصادرة عنها أثناء الكتابة، وكل الصفات الطبيعية والسلوكية للإنسان وغيرها من الصفات الجسدية الأخرى [2].

أما عن آلية إنشاء التوقيع البيومتري، فإنه يسند لجهة معينة مهمة أخذ صورة دقيقة لصفة ذاتية للشخص الذي يرغب في استخدام التوقيع البيومتري، وذلك عن طريق تقنية مخصصة لذلك، ثم يتم حفظ هذه الصورة بعد تشفيرها في ذاكرة الحاسوب. وعند إبرام التصرف يتم التأكيد من مطابقة سمات الشخص المحفوظة عنه من قبل باستخدام برنامج خاص[3].

بالرغم من مزايا هذا النوع من التوقيع، باعتباره قائم على الخواص الذاتية المنفردة للإنسان والتي لا تتشابه إكلينيكيا، مما يجعلها تتميز بدرجة عالية من الموثوقية[4]، إلا أن بعض

---

(1) – **عزيزة لرقط**، الحماية الجنائية للتوقيع والتصديق الإلكترونيين في التشريع الجزائري، مجلة الاجتهاد للدراسات القانونية والاقتصادية، العدد 11، جانفي 2017، ص 108.

(2) – **رشيدة بويكر**، التوقيع الالكتروني في التشريع الجزائري (دراسة مقارنة)، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 04، ديسمبر2016، ص71، وأنظر أيضا: **حمودي ناصر**، مرجع سابق، ص338؛ **يوسف أحمد النوافلة**، مرجع سابق، ص96، **عزيزة لرقط**، مرجع سابق، ص108؛ **مصطفى هنشور وسيمة**، مرجع سابق، ص 413.

(3) – **سعدي الربيع**، حجية التوقيع الالكتروني في التشريع الجزائري، أطروحة مقدمة لنيل درجة الدكتوراه في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة باتنة –1– ، 2016، ص62؛ **سعيد السيد قنديل**، التوقيع الالكتروني، ماهيته، صوره، حجيته في الإثبات بين التدويل والاقتباس، دار الجامعة الجديدة للنشر، مصر،2004، ص70.

(4) – **حسن عبد الباسط جميعي**، مرجع سابق، ص41، **علاء محمد نصيرات**، مرجع سابق، ص32.

الفقه[1]، أورد بعض التحفظات على هذا النوع من التوقيع لإمكانية نسخ صورة منه كنسخ ذبذبات الصوت وبصمة الإصبع، وصنع عدسات للعين مطابقة لقزحية العين أو طلاء الشفاه أو الإصبع بمادة تجعلها مطابقة للبصمة الأصلية.

- احتمال تغيير بعض خصائص الإنسان بفعل الظروف، كتآكل بصمات الأصابع عبر الزمن، أو تأثير التوتر على نبرة الصوت ...الخ.
- إن الاحتفاظ بصورة التوقيع داخل القرص الصلب للحاسوب يجعلها عرضة للنسخ أو القرصنة مما يضعف قيمتها في الإثبات[2].

تجدر الإشارة إلى أن المشرع الجزائري استعمل هذا التوقيع في إصدار بطاقة التعريف وجواز السفر البيومتريين بموجب القرار المؤرخ في (19 جويلية 2010) يتعلق بملف طلب بطاقة التعريف وجواز السفر البيومتريين وكيفيات معالجته[3]، وهذا استجابة لدعوة المنظمة العالمية للطيران إلى إصدار جواز سفر بيومتري.

ثالثا: التوقيع الكودي

يعرف هذا التوقيع أيضا باسم التوقيع باستخدام الرقم السري والبطاقة الممغنطة، ويعتبر أول شكل أظهرته التقنيات التكنولوجية للتوقيع الالكتروني وهو الأكثر شيوعا[4]. لذا استحدث هذا الشكل من التوقيع الالكتروني من أجل الإسراع في إنجاز المعاملات البنكية؛ يعتبر القطاع المصرفي المجال الأكثر استعمالا لمثل هذا النوع من التوقيعات، خاصة في عمليات السحب

---

(1) – **ثروت عبد الحميد**، مرجع سابق، 60؛ **نجوى أبو هيبة**، مرجع سابق، ص ص50 –51.

(2) – **فتحي بن جديد**، مدى حجية الكتابة والتوقيع الالكترونيين في إثبات العقد المبرم عبر الانترنت، مجلة دراسات قانونية، مركز البصيرة للبحوث والاستشارات والخدمات التعليمية، الجزائر ع 16، 2013، ص113؛ أنظر أيضا **يوسف زروق**، حجية التوقيع الالكتروني في الإثبات، دراسة مقارنة، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور، الجلفة،ع 06، 2010، ص188.

(3) – قرار مؤرخ في 07 شعبان عام 1431 الموافق 19 يوليو سنة 2010، يتعلق بملف طلب بطاقة التعريف الوطنية وجواز السفر البيومتريين الالكترونيين وكيفيات معالجته، ج.ر.ع 45، صادر بتاريخ 8 غشت 2010.

(4) – **عيسى غسان ربضي**، مرجع سابق، ص58؛ **يوسف أحمد النوافلة**، مرجع سابق، ص93.

النقدي من حساب الشخص[1]. كما يوجد نوع أخر من البطاقات الممغنطة تمكن صاحبها من تسديد ثمن مشترياته أو مقابل ما يحصل عليه من خدمات عن طريق أجهزة دفع مخصصة، كما يمكن بالدفع عن طريق هذه البطاقات عبر الانترنت[2].

أما عن آلية العمل بهذا التوقيع، فتتم بإدخال الموقِّع لبطاقته الممغنطة إلى الجهاز الآلي (سواء كان صراف آلي، أو جهاز الدفع الالكتروني)، ثم يقوم بعد ذلك بإدخال الرقم السري الخاص به عن طريق لوحة المفاتيح، ثم الضغط على الأمر بالموافقة على إتمام العملية[3].

بعد تمام عملية السحب، يصدر الجهاز الآلي شريط ورقي يبين فيه تاريخ ووقت إجراء العملية، قيمة المبلغ المسحوب وقيمة المبلغ المتبقي في رصيد العميل [4].

ثار جدل فقهي حول مدى صحة التوقيع الكودي بين معارض و مؤيد؛ إذ يرى الفريق الأول أن هذا التوقيع لا يستوف الوظائف الأساسية للتوقيع، حيث يبررون رفضهم لهذا التوقيع بأنه لا يحدد هوية المستخدم الفعلي للبطاقة؛ إذ يمكن الاستيلاء على البطاقة والرقم السري الخاص بها[5]. في حين يرى الفريق الثاني من الفقهاء[6]، صلاحية هذا التوقيع وقدرته على تحديد هوية صاحبه وتمتعه بالثقة والأمان وذلك كالآتي:

1- إن استعمال العميل للبطاقة الممغنطة مع الرقم السري يعتبر إقرارا منه بما يريد من بيانات الشريط الناتج عن الجهاز الآلي.

---

(1) – **عائشة قصار الليل**، مرجع سابق، ص103.

(2) – **كريم لملوم**، الإثبات في معاملات التجارة الالكترونية بين التشريعات الوطنية والدولية، مذكرة لنيل درجة الماجستير في القانون، فرع قانون التعاون الدولي، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2011، ص128؛ انظر كذلك **سهيلة طمين**، الشكلية في عقود التجارة الالكترونية، مذكرة لنيل درجة الماجستير في القانون فرع القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو 2011، ص 58 وما يليها.

(3) – **حسن عبد الباسط جميعي**، مرجع سابق، ص36؛ **عائشة قصار الليل**، المرجع نفسه، ص104.

(4) – **ثروت عبد الحميد**، مرجع سابق، ص57.

(5) – **محمد فواز المطالقة**، مرجع سابق، ص 183؛ **سعيد السيد قنديل**، مرجع سابق، ص 68.

(6) – **سعيد السعيد قنديل**، المرجع نفسه، ص60؛ **حسن عبد الباسط جميعي**، المرجع نفسه، ص36.

2- إن سرقة البطاقة الممغنطة لا يعني الحصول على الرقم السري، لانفصالهما عن بعض. أما إمكانية حدوثهما معا فهو أمر نادر الحدوث، وفي هذه الحالة يطلب العميل وقف العمل بها.

3- كل الأجهزة الخاصة بالسحب أو الدفع الآلي مبرمجة على رفض البطاقة بعد المحاولة الثالثة لإدخال الرقم السري، مما يضيق فرص استعمالها بالطرق غير الشرعية.

ساند القضاء الفرنسي الاتجاه الثاني للفقه، حيث اعترفت الغرفة المدنية الأولى لمحكمة النقض الفرنسية بتاريخ (08 نوفمبر 1989)، بالتوقيع الكودي ومنحته الحجية في الإثبات، كونه محاط بالضمانات نفسها المقررة للتوقيع التقليدي، واستند في إضفاء الحجية له على الاتفاقات التي تبرم بين ذوي الشأن [1].

تجدر الإشارة إلى أن المشرع الجزائري قد واكب هذه التطورات من خلال اعترافه بهذا النوع من التوقيعات، وذلك بموجب المادة (543) من القانون التجاري الجزائري حيث قسّم البطاقات إلى نوعين؛ بطاقات دفع وبطاقات سحب تصدرها البنوك أو الهيئات المالية المؤهلة قانونا لذلك؛ وذلك بنصها: «**تعتبر بطاقات دفع كل بطاقة صادرة عن البنوك والهيئات المالية المؤهلة قانونا وتسمح لصاحبها بسحب أو تحويل الأموال.**

تعتبر بطاقة سحب كل بطاقة صادرة عن البنوك والهيئات المالية المؤهلة قانونا وتسمح لصاحبها فقط بسحب الأموال».

كما أن المادة (69) من قانون النقد والقرض رقم (03-11) [2]، التي تنص على: «**تعتبر وسائل الدفع كل الأدوات التي تمكن من تحويل أموال مهما يكن السند أو الأسلوب**

(1) – Cass, chambre civil 1, du 08 novembre1985, 86 -16 – 197 publie au bulletin 1989 in 342 p 230.

(2) – الأمر رقم 03-11 المتعلق بالنقد و القرض المؤرخ في 26 أوت 2003، ج.ر.ع 552، صادر في 27 أوت 2003، المعدل والمتمم بالأمر رقم 09-01، المؤرخ في 22 جويلية 2009، المتضمن قانون المالية لسنة 2009، ج .ر.ع 44 صادر بتاريخ 26 جويلية 2009، المعدل والمتمم بالأمر رقم 10-04 المؤرخ في 26 أوت 2010، المتضمن تعديل الأمر رقم 03-11 ج.ر.ع 50 صادر بتاريخ 01 سبتمبر 2010، متمم بالقانون رقم 13-08 المؤرخ في 30 ديسمبر 2013،=

التقني المستعمل»، مما يجعل هذا النص يستوعب كل تقنيات ووسائل الدفع، بما في ذلك البطاقة المغناطيسية.

اتّسع التّعامل بالبطاقات الممغنطة في المعاملات المالية والمبادلات النّقدية، وقد أصدرت الشّركة الجزائرية للمبادلات النّقدية فيما بين البنوك المسماة "SATIM" [1] هذه البطاقات التي تسمى ببطاقات الائتمان، بحيث تمكن هذه البطاقة حاملها من سحب واستلام النقود عن طريق الموزع الإلكتروني (D.A.B)[2]، أو بواسطة الشباك البنكي الإلكتروني (G.A.B)[3]، كما يسمح له أيضا بسداد ثمن السلع والخدمات وباقي المستحقات مقابل المعاملات التي يجريها في المجال التجاري.

رابعا: التوقيع بالقلم الالكتروني

يعتبر هذا النوع من التوقيع الإلكتروني من بين صور التوقيع الالكتروني التي يمكن استخدامها في توثيق التصرفات القانونية المبرمة عبر الوسائط الالكترونية، حيث يتم التوقيع

=المتضمن قانون المالية لسنة 2014، ج. ر.ع 68 صادر بتاريخ 31 ديسمبر 2013، المعدل بموجب القانون رقم 16-14 المؤرخ في 28 ديسمبر 2016 المتضمن قانون المالية لسنة 2017، ج.ر .ع 77 صادر بتاريخ 29 ديسمبر 2016.

(1)- (**S.A.T.I.M.: Société Algérienne des transactions interbancaire et monétaire.**) – شركة تألية الصفقات البنكية المشتركة والنقدية، تم إنشاءها في مارس (1996) برأسمال قدره (257) مليون دج، كشركة يساهم فيها (8) بنوك تجارية: بنك الجزائر الخارجي، بنك الفلاحة والتنمية الريفية، البنك الوطني الجزائري، بنك التنمية المحلية، الصندوق الوطني للتوفير والاحتياط، بنك البركة الجزائري، القرض الشعبي الجزائري، الصندوق الوطني للتعاون الفلاحي. لأجل الاهتمام بتقنية المعلومات وتطوير وتسيير نظام نقدي بين البنوك منخفض التكلفة، فضلا عن تنظيم وتحديث أنشطة البنوك وإصلاحها من خلال ترقية أداء الخدمات ذات الصلة بتحديث وسائل الدفع وإصدار النقود الالكترونية، وتتمثل المهام الرئيسية لهذه الشركة:

- تطوير وتوسيع استعمال وسائل الدفع الالكتروني: وذلك من خلال إصدار البطاقات البنكية وإدخالها كوسيلة سحب ودفع بين البنوك.
- تنظيم العلاقة بين البنوك: من خلال تامين قبول البطاقات لدى كل البنوك المساهمة وإجراء المقاصة بينها.
- التكفل بالهياكل القاعدية التكنولوجية، وذلك من خلال التجهيز بالموزعات الآلية للنقد وصيانتها.

نقلا عن: **سمية دميش**، التجارة الالكترونية حتميتها وواقعيتها في الجزائر، مذكرة لنيل شهادة الماجستير في العلوم الاقتصادية، كلية العلوم الاقتصادية وعلوم التسيير، جامعة منتوري، قسنطينة، 2011، ص 260.

)-2(D.A.B.: Distributeur automatique des billets.

)-3(G.A.B.: Guichet automatique de banque.

بهذه الصورة عن طريق استخدام قلم إلكتروني حسابي (Pen–op) يمكن من خلاله الكتابة على شاشة الحاسوب[1].

تتم آلية تشغيل منظومة التوقيع بالقلم الالكتروني عن طريق تثبيت برنامج خاص يعرف بمصطلح (دينمو) على قاعدة بيانات الحاسوب المتصل به القلم الالكتروني، إذ يقوم هذا البرنامج بوظيفتين أساسيتين وهما:

– وظيفة التقاط التوقيع، ووظيفة التحقق من صحة التوقيع[2]، وسنتعرض بالشرح لكل وظيفة منهما على حدى:

1 – الوظيفة الأولى: وظيفة التقاط التوقيع

بداية يضع المُوقع كل بياناته كالاسم والجنس والعمر والوظيفة في البرنامج الموجود على حاسوبه عن طريق بطاقته الخاصة، بعد إدخال هذه البيانات تظهر تعليمات على الشاشة لينفذها الموقع، بمجرد تنفيذها تظهر تعليمات أخرى مفادها أنه "على الشخص المستخدم كتابة توقيعه داخل المربع الذي سيظهر على الشاشة باستخدام القلم الالكتروني". عند الانتهاء من كتابة التوقيع يرى المُوقع توقيعه على شاشة الحاسوب بذات الشكل الذي كتبه به، عندئذ يقوم البرنامج بقياس خصائص معينة من حيث الحجم، الشكل، النقاط، الخطوط، الالتواءات، درجة الضغط على القلم، ليظهر بعد ذلك على الشاشة خيار موافق أو غير موافق، فإذا تمت

(1) – **رايس محمد**، حجية الإثبات بالتوقيع الإلكتروني طبقا لقواعد القانون المدني الجزائري الجديد، المجلة الجزائرية للقانون المقارن، العدد 01، 2018، ص37؛ أنظر أيضا: **وسن كاظم زرزور**، التوقيع الالكتروني كدليل من أدلة الإثبات في ضوء أحكام قانون الإثبات العراقي رقم (107) لسنة 1979 المعدل، مجلة رسالة الحقوق، العدد الثاني، السنة الثالثة، العراق، 2011، ص144.

(2) – **عيسى غسان ربضي**، مرجع سابق، ص 64.

الموافقة، يجمع البرنامج كل البيانات المُخزنة ويدمجها مع التوقيــع، ثم يقوم بتشفيرها والاحتفاظ بها لحين الحاجة إليها[1].

2- الوظيفة الثانية: التحقّق من صحة التوقيع

عند الحاجة إلى التوقيع مرة أخرى، يطلب البرنامج الخاص بالتوقيع من الشخص إعادة كتابة توقيعه داخل المربع المخصص لذلك، هنا تبدأ الوظيفة الثانية للبرنامج، أين يجري مقارنة بين خصائص التوقيع المُدخل مع التوقيع المحفوظ سابقا، ثم يقدم تقريرا بالنتيجة على أساس نسبة التطابق التي سجلها [2].

ما يميّز هذا التوقيع؛ هو إمكانية التحقّق من التوقيع في كل مرة يتم التوقيع فيها. لكن يؤخذ عليه تكلفته الباهظة جدا، إضافة إلى حاجته الدائمة لأجهزة مرفقة بجهاز الحاسوب وهي غير متوفرة دائما. كما أن استخدامه عبر الانترنت سيحتاج إلى وجود طرف ثالث موثوق يضمن عدم التلاعب به أو تزويره[3].

لكن يجب التنبيه إلى وجوب التفرقة بين التوقيع بالقلم الالكتروني السالف الذكر والتوقيع بالماسح الضوئي، إذ أن هذا الأخير يقوم على نقل التوقيع المحرر بخط اليد عن طريق التصوير بالماسح الضوئي (Scanner)، ثم نقل صورة التوقيع إلى جهاز الحاسوب، وإضافتها إلى الملف المراد التوقيع عليه[4]. إذ لا ترقى هذه الصورة إلى المستوى الذي تعد فيه من صور

---

(1) – **عيسى غسان ربضي**، مرجع سابق، ص65؛ **فوغالي بسمة**، اثبات العقد الالكتروني وحجية في ظل عالم الانترنت، مذكرة لنيل شهادة الماجستير في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة محمد لمين دباغين، سطيف-2- ، 2014-2015، ص72.

(2) – **سليماني مصطفى**، مرجع سابق، ص273.

(3) – **أبو الليل إبراهيم الدسوقي**، التوقيع الالكتروني ومدى حجيته في الإثبات "دراسة مقارنة"، بحث مقدم لمؤتمر القانون والحاسوب المنعقد من 12 إلى 14 تموز 2004، كلية الحقوق، جامعة اليرموك، الأردن، ص06.

(4) – **ناصر حمودي**، مرجع سابق، ص341، **حسن عبد الباسط جميعي**، مرجع سابق، ص35.

التوقيع الالكتروني، لما يعتريها من خطر التزوير، وعدم توفر عنصر الأمان والثقة بها؛ لذا استقر الفقه القانوني على عدم الاعتداد بحجية التوقيع بالماسح الضوئي في الإثبات[1].

نصل في الأخير إلى أنه كلما كان التوقيع الإلكتروني قائما على شهادة تصديق إلكترونية تقدمها جهات التصديق الإلكتروني، كلما كان أكثر موثوقية، وحقق الأمن والسرية المتطلبان فيه، وذلك بالتأكيد على وظائف التوقيع؛ من تحديد لهوية الموقع ورضائه بما وقع عليه.

الفرع الثاني
مدى تحقق وظائف التوقيع في صور التوقيع الإلكتروني

يحصر أغلب الفقهاء وظائف التوقيع التقليدي في وظيفتين أساسيتين يؤديهما في الإثبات، تتمّثل الأولى في تحديد هوية الموقع، أما الثانية فتتمّثل في مدى التزامه بما وقع عليه[2]. وتعتبران الوظيفتين الأساسيتين الواجب توافـــرهما في صور التوقيــع الالكتـروني، حتى يحقق هذا الأخير الغاية الأساسية من إنشائه؛ ألا وهي إضفاء القوة الثبوتية على التصرفات القانونية، وهو ما درج المشرع الجزائري على تأكيده حينما حدّد وظائف التوقيع الإلكتروني في الباب الثاني من القانون (15-04) سالف الذكر، حيث نص في المادة (6) منه: «**يستعمل التوقيع الالكتروني لتوثيق هوية الموقع وإثبات قبوله مضمون الكتابة في الشكل الإلكتروني**».

غير أن ما أفرزته التكنولوجيا الحديثة من صور مستحدثة للتوقيع الإلكتروني، كشف عن وظيفة جديدة، تتمثل في سلامة محتوى ما تم التوقيع عليه، وتعتبر بمثابة ضمان إضافي يضفي الثقة على المعاملات الإلكترونية [3].

---

(1) – **قنديل سعيد السيد**، مرجع سابق، ص66؛ **عائشة أراميس**، الإثبات في العقود الالكترونية المبرمة عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون، كلية الحقوق، جامعة يوسف بن خدة، بن عكنون، 2007، ص92.

(2) – **توفيق حسن فرج**، قواعد الإثبات في المواد المدنية والتجارية، دار الثقافة الجامعية، الإسكندرية، 1981، ص103؛ **محمود عبد الرحيم الشريفات**، التراضي في تكوين العقد عبر الانترنت، دار الثقافة للنشر والتوزيع، الأردن، ط1، 2009، ص197.

(3) – **يوسف أحمد النوافلة**، الإثبات الالكتروني في المواد المدنية و المصرفية ، مرجع سابق، ص102.

وعليه سنبين من خلال هذا الفرع الوظائف المختلفة التي يؤديها التوقيع الإلكتروني في الإثبات ومدى قدرة كل صورة من صوره على تحقيقها.

أولا: تحديد هوية الموقع

تعتبر تحديد هوية الموقع في التوقيع التقليدي أمرا سهلا؛ نظرا للحضور المادي للأطراف لحظة التوقيع، إضافة إلى أنه غالبا ما يتم إلزامهم بتقديم وثائق التعريف بهويتهم من قبل الموظف القائم على إبرام التصرف القانوني، وهذا ما يختلف كليا بالنسبة للتوقيع الإلكتروني الذي يتم عبر وسائط إلكترونية غير ملموسة تجعل من الصعب تحديد هوية الموقع إلكترونيا[1].

لا يتعلق الشرط الجوهري في التوقيع بالاتصال المادي بين التوقيع في ذاته وصاحبه، وإنما يتعلق بقدرته؛ أيا كان شكله أو وسيلة إصداره؛ على تحديد هوية صاحبه وتمييزه عن غيره. وهذا ما اشترطته العديد من تشريعات الإثبات الإلكتروني وعلى رأسها قانون اليونسترال النموذجي بشأن التجارة الالكترونية لعام (1996)؛ حيث نص في مادته (7) المعنية بتحديد مصطلح التوقيع على أنه:« **عندما يستلزم القانون توقيع شخص ما (على المحرر) فإن رسالة البيانات تعتبر مستوفية لهذا الشرط إذا:**

أ)- استخدمت طريقة لتحديد هوية ذلك الشخص والتدليل على موافقته على المعلومات الواردة ضمن رسالة البيانات؛

ب)- إذا كانت تلك الطريقة جديرة بالتعويل عليها بالقدر المناسب للغرض الذي أنشئت أو بلغت من أجله رسالة البيانات وفي ضوء كل الظروف ».

كما نص المشرع الفرنسي في المادة (1367) من الأمر (2016-131) المتعلق بإصلاح العقود وإثبات الالتزامات على أن: «التوقيع **اللازم للاعتداد بالتصرف القانوني يحدد هوية مصدره، ويعبر عن قبول الأطراف بالالتزامات المترتبة عن هذا التصرف...**». ثم أضاف

---

(1) - عرف المشرع الجزائري الموقع الالكتروني في نص المادة 2 ف 2 من القانون 15-04 بأنه: «**شخص طبيعي يحوز بيانات إنشاء التوقيع الالكتروني ويتصرف لحسابه الخاص أو لحساب الشخص الطبيعي أو المعنوي الذي يمثله**».

في الفقرة الثانية «**... عندما يكون التوقيع إلكترونيا، فانه يتمثل في استخدام وسيلة موثوق بها لتحديد الشخص تضمن صلته بالتصرف الذي وقع عليه...**».

أما عن المشرع الجزائري، فقد أشار في المادة (327) من القانون المدني الجزائري على أنه: «**... ويعتد بالتوقيع الالكتروني وفق الشروط المذكورة في المادة 323 مكرر 1 أعلاه**»، وبالعودة لنص المادة (323 مكرر 1)[1] من القانون المدني الجزائري نجدها تنص على شروط الكتابة الإلكترونية والتي من بينها تحديد هوية الشخص الذي أصدرها.

كما أكد المشرع الجزائري على ذلك من خلال نص المادة (6) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين، بنصها على أنه: «**يستعمل التوقيع الإلكتروني لتوثيق هوية الموقع وإثبات قبوله مضمون الكتابة في الشكل الإلكتروني**».

عند استقراء كل هذه النصوص القانونية، نجد أنها تشترط إلزامية تحديد هوية الموقع في التوقيع الإلكتروني حتى يتمتع بالحجية في الإثبات. أما إذا لم يكن التوقيع كاشفا عن هوية صاحبه، فإنه لا يعتد به، ويصير قاصرا عن أداء دوره في إسباغ الحجية على المحرر، وذلك لقطع الطريق على منتحلي الشخصيات وعلى من هم دون سن الأهلية القانونية[2].

أما بالنسبة للفقه؛ فيرى جانبا منه[3]؛ أن التوقيع الذي يتم عبر الانترنت باستخدام إشارات أو رموز، يعتبر بمثابة توقيع بالختم، وتتحقق به -بالتالي- حجية الورقة الممهورة بالتوقيع الإلكتروني. وعليه؛ فإن الادعاء باستخدام هذه البيانات بدون رضا صاحبها، يجب أن يتم عن طريق الطعن بالتزوير، أين يقع عبء الإثبات على عاتق المدعي، وهذا ما يتوافق مع الأحكام

---

(1) - تنص المادة (323 مكرر 1) من القانون المدني الجزائري على أنه: «**يعتبر الإثبات بالكتابة في الشكل الالكتروني كالإثبات بالكتابة على الورق، بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها**».

(2) - **حسن عبد الباسط جميعي**، مرجع سابق، ص45؛ **علاء محمد نصيرات**، مرجع سابق، ص68.

(3) - **أحمد شوقي محمد عبد الرحمن**، النظرية العامة للالتزام، أحكام الالتزام والإثبات في الفقه وقضاء النقض، النسر الذهبي للطباعة، مصر، 2004، ص ص363، 364.

المقررة بالخصوص في حال التوقيع عن طريق الختم، غير أن الختم في هذه الحالة هو عبارة عن ختم رقمي مشفر[1].

وضّحنا فيما سبق أن التوقيع الالكتروني قائم على مجموعة من الأرقام أو الإشارات أو الرموز أو العلامات ...، غير أنه من الضروري أن نتساءل كيف يمكن لهذه الرموز أو الحروف أو الأرقام أو غيرها من الإشارات غير الملموسة المنشأة على وسيط إلكتروني أن تحدد هوية صاحبها؟

بالعودة إلى مختلف صور التوقيع الإلكتروني التي تطرقنا إليها من قبل، نجدها تتفاوت في قدرتها على تحديد هوية الموقع. فهناك من أشكال التوقيع الإلكتروني الذي يفتقد للمصداقية كالتوقيع الذي يتم بواسطة الضغط على أحد مفاتيح الحاسوب بما يفيد الموافقة، أو التوقيع بالماسح الضوئي، إذ يقوم هذا التوقيع على نقل الصورة الفوتوغرافية للتوقيع العادي على قاعدة بيانات الحاسوب ليوضع بعدها على المحرر الإلكتروني، مما يسهل نسخه من قبل الغير واستعماله بغير علم صاحبه دون أن يترك ذلك أي أثر.

لذا أجمع الفقهاء على اعتباره من التوقيعات التي لا تحدد هوية صاحبها [2]. ومن أشكال التوقيع الإلكتروني التي تتوقف قدرته في تحديد هوية صاحبها على نوعية وحداثة التقنية المستعملة في تشغيل منظومتها نجد:

التوقيع البيومتري:

إن اعتماد هذا التوقيع على السمات الفيزيائية للإنسان التي تتمتع بقدر عالي من الاستمرارية والثبات، والتي تختلف من شخص لآخر، تتيح له تحديد هوية الموقع بصورة مؤكدة، إلا أن هذه الإمكانية تبقى مرهونة بمدى موثوقية النظام المعلوماتي الذي يمكّن المستخدمين من حماية توقيعاتهم من الاختراق والنسخ والتزوير[3]. وهذا ما يجعل التوقيع

---

(1) – **بلحاج بلخير**، مرجع سابق، ص449.

(2) – **عيسى غسان ربضي**، مرجع سابق، ص ص90، 91؛ **علاء محمد نصيرات**، مرجع سابق، ص69.

(3) – **باهة فاطمة**، مرجع سابق، ص164؛ **يوسف أحمد النوافلة**، الإثبات الالكتروني في المواد المدنية والمصرفية، مرجع سابق، ص98.

البيومتري مكلفا للغاية، مما أدى إلى محدودية انتشاره، لذا يقتصر استعماله حاليا على قطاعات معينة في الدولة أو في البنوك الكبرى[1].

التوقيع بالقلم الالكتروني:

تتوقف قدرة هذا النوع من التوقيع في تحديد هوية صاحبه على التقنية المستخدمة في إنشائه، فالتوقيع بهذا الشكل يحتاج إلى حاسوب مزوّد بوحدة القلم الإلكتروني الخاصة به، وكلما كانت هذه الأخيرة مؤمنة من الاختراق، كلما تمكّن هذا التوقيع من تحديد هوية الموقع. لذا لابد من أن تكون التقنية المستخدمة في التوقيع بالقلم الإلكتروني ذات درجة عالية من الأمان[2].

أما عن أشكال التوقيع الالكتروني التي لها القدرة على تحديد هوية أصحابها بشكل مساو للتوقيع التقليدي فنجد:

التوقيع باستخدام البطاقة الممغنطة المقترنة بالرقم السري:

يتميز هذا التوقيع بسهولته وبساطة منظومته، حيث يوفر قدرا كبيرا من الأمان بسبب سرية التعامل بالرقم السري، كما أنه يمكن السيطرة على الرقم السري في حال فقده أو سرقته، هذا ما جعل الفقه يجمع على صلاحيته وقدرته على تحديد هوية صاحبه، دون أن نغفل أنه قد حاز على اعتراف القضاء بحجيته القانونية الكاملة في الإثبات[3].

---

(1) – **زروق يوسف**، حجية وسائل الإثبات الحديثة، رسالة مقدمة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2013/2012، ص 250.

(2) – **علاء حسين مطلق التميمي**، الدليل الالكتروني في الإثبات المدني، دراسة مقارنة، ط1، دار النهضة العربية، مصر، 2010، ص202؛ **محمد رضا أزرو**، مرجع سابق، ص180؛ **علاء محمد نصيرات**، مرجع سابق، ص74.

(3) – Cass, chambre civil 1, du 08 novembre1989 , op.cit.

التوقيع الرقمي:

إن هذا التوقيع يوّفر أعلى درجات الضمان، إذ أنه يحّدد هوية صاحبه دون أدنى مجال للشك، وذلك راجع إلى أنه يقوم على تقنية التشفير (المفتاحين العام والخاص). حيث يقوم بتشفير التوقيع والمحرر الالكترونيين ويحولهما إلى معادلات خوارزمية معقدة لا يمكن فكها أو تزويرها أو اختراقها إلا إذا فقد الشخص سيطرته على المفتاح الخاص[1]، فضلا عن وجود جهات التصديق التي تقوم بإصدار شهادات تصديق إلكترونية لإثبات صحة التوقيع الإلكتروني[2].

ثانيا: قدرة التوقيع الإلكتروني على إثبات قبول الموقع على مضمون المحرر الإلكتروني

لا يختلف الأمر بالتعبير عن الإرادة في الالتزام بمحتوى التصرف القانوني عما هو في تحديد هوية الشخص، نظرا للارتباط الوثيق بين الوظيفة الأولى للتوقيع والمتمثلة في تحديد هوية الموقع وهذه الوظيفة الثانية والمتعلقة بالتعبير عن إرادته[3]. إذ يمكن القول أنه كلما كانت صور التوقيع الإلكتروني غير قادرة على تحديد هوية الموقع، كلما كانت عاجزة عن التعبير عن إرادته. حيث أن الأمر في الحالتين معلّق على حداثة التقنية التكنولوجية المستخدمة وقدرتها على توفير الأمان والسرية، فكلما كانت هذه التقنية قادرة على توثيق الرابطة القائمة بين التوقيع والمحرر، كلما كان لها القدرة على التعبير عن إرادة الموّقع في الالتزام بما وقع عليه[4].

وبالرجوع إلى أشكال التوقيع الإلكتروني، نجد أن التوقيع بالماسح الضوئي لا يمكنه تحقيق هذه الوظيفة لأنه غير قادر أصلا على تحديد هوية الموّقع كما بينا سابقا.

---

(1) – **محمد محمد سادات**، حجية المحررات الموقعة إلكترونيا، مرجع سابق ص 193.

(2) – سيتم التطرق إلى جهات التصديق الالكتروني وشهادات التصديق الالكترونية بالتفصيل في الباب الثاني من هذه الأطروحة.

(3) – **باهة فاطمة**، مرجع سابق، ص166؛ **عائشة قصار الليل**، مرجع سابق، ص142؛ **علاء محمد نصيرات**، مرجع سابق، ص72.

(4) – **عيسى غسان ربضي**، مرجع سابق، ص91؛ **مليكة مراد**، مرجع سابق، ص84.

أما بالنسبة للتوقيعين البيومتري والقلم الإلكتروني، فبمجرد أن يقوم الموّقع بتطبيق أحد هذين التوقيعين فإن ذلك يعتبر تعبيرا عن موافقته على ما وَّقع عليه، شرط أن تكون التقنية المستخدمة ذات كفاءة عالية [1].

الأمر ذاته بالنسبة للتوقيع الكودي (البطاقة الممغنطة المرتبطة بالرقم السري)، إذ أن إدخال الموقع لبطاقته في جهاز الصراف الآلي وإدخاله للرقم السري الخاص به، ثم اتباعه للتعليمات المطلوبة دليل قاطع على موافقته على مضمون العملية المراد إتمامها دون أدنى شك، إذ لا يمكن لأحد أن يعبّر عن إرادته بدلا عنه إلا إذا حاز على البطاقة وكان عالما بالرقم السري، وهو أمر نادر الحدوث إلا في حالة الإهمال الشديد[2].

ويبقى التوقيع الإلكتروني الرقمي الصورة الوحيدة التي تحقق الارتباط القوي بين الموقّع ومحتوى المحرر الإلكتروني. إذ أن اعتماده على تقنية التشفير اللاتماثلي تمنح للموّقع دون سواه القدرة على تعديل مضمون المحرر، إضافة إلى وجود جهات التصديق والتي تقوم في كل مرة بتأكيد صحة التوقيع.

ثالثا: قدرة التوقيع الإلكتروني على التحقّق من سلامة محتوى ما تم التوقيع عليه

إن انتقال المحرر الإلكتروني بين أطراف المعاملة الإلكترونية عبر فضاء إلكتروني مفتوح ومتاح للجميع، يعرضه للكثير من المخاطر (القرصنة)، مما يثير التساؤل حول ما إذا كان مضمون المحرر المرسل هو ذات المحرر المستقبل. لذا استحدث الفقه والقانون وظيفة جديدة للتوقيع الإلكتروني؛ وهي ضمان سلامة المحرر الموقع إلكترونيا. فالاعتراف بسلامة التوقيع الإلكتروني يستلزم خلو بيانات المحرر الإلكتروني من أي تعديل أو تحريف؛ سواء بالحذف أو بالإضافة؛ وذلك أثناء إنشائه أو نقله أو إرساله أو حفظه أو استرجاعه، وبصرف النظر عما إذا كان التعديل عمدي أو غير عمدي[3].

---

(1) – **بلقنيشي الحبيب**، مرجع سابق، ص132.

(2) – **علاء محمد نصيرات**، مرجع سابق، ص72 وما يليها.

(3) – **بلقاسم عبد الله**، مرجع سابق، ص123؛ **المعتصم بالله فوزي أدهم**، مرجع سابق، ص346.

والتوقيع الإلكتروني هنا لا يضفي حجية على سلامة المحرر وصحته، وإنما قرينة تقبل إثبات العكس على سلامة مضمون المحرر من أي تعديل أو تبديل؛ إذ أنه حتى ولو ثبتت سلامة المحرر من أي تعديل، فإنه من الممكن إثبات عدم حجية المحرر الإلكتروني أو بطلانه أو صوريته[1].

تتحّقق هذه الوظيفة بصورة مطلقة على الدعامة الورقية الممهورة بتوقيع تقليدي، لأن أي محاولة للكشط أو التزوير تترك أثرها على الحامل الورقي، إذ يمكن اكتشافه بسهولة؛ سواء عن طريق المناظرة أو من طرف خبير في حالة التزوير المتقن، بالإضافة إلى ذلك فان الدعامة الورقية تتميز بطابعها المادي الذي يضمن عدم المساس بمضمون ما تم التوقيع عليه[2].

إلا أن الأمر يختلف في البيئة الإلكترونية القائمة على دعامة إلكترونية لا مادية، أين تتفاوت صور التوقيع الإلكتروني فيما بينها من حيث تحقيق هذه الوظيفة، وذلك راجع بالأساس إلى جدارة النظام التقني المنشئ لها ومدى قدرته على حفظها وحمايتها من الاختراق.

إلا أن التوقيع الرقمي القائم على تقنية التشفير، يبقى التوقيع الإلكتروني الوحيد وبدون منازع القادر على تحقيق وظائف التوقيع كلها، وذلك عن طريق عملية رياضية يطلق عليها «دوال أو اقترانات التمويه» التي يتم من خلالها إنشاء شكل مضغوط من المحرر الإلكتروني، يشار إليه بوجه عام "بالبصمة الالكترونية للمحرر الالكتروني"[3]، ولا يمكن

---

(1) – **يوسف أحمد النوافلة**، الإثبات الالكتروني في المواد المدنية والمصرفية، مرجع سابق، ص101؛ **سليماني مصطفى**، مرجع سابق، ص252.

(2) – **حابت أمال**، التجارة الالكترونية في الجزائر، رسالة لنيل شهادة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2015، ص115؛ أنظر كذلك؛ **بلحاج بلخير**، مرجع سابق، ص458.

(3)– **البصمة الإلكترونية للمحرر** هي بصمة رقمية يتم اشتقاقها وفقا لخوارزميات معينة تدعى "دوال أو اقترانات التمويه"، إذ تُطبق هذه الخوارزميات حسابات رياضية على المحرر لتوليد بصمة (سلسلة صغيرة) تمثل ملفا كاملا أو رسالة، وتدعى البيانات الناتجة "البصمة الإلكترونية للمحرر".

تتكون البصمة الإلكترونية للمحرر من بيانات لها طول ثابت (يتراوح عادة ما بين 128 و160 بت)، تؤخذ من المحرر المُحول ذات الطول المتغير. وتستطيع هذه البصمة تمييز المحرر الأصلي والتعرف عليه بدقة، حتى إن أي تغيير فيه – ولو كان في بت واحد– سيفضي إلى بصمة مختلفة تماما. =

فهمها ولا قراءتها إلا باستخدام مفتاح معيّن، وأي تغيّر يطرأ على المحرر تترتب عليه دائما بصمة إلكترونية مختلفة عندما يستخدم نفس «اقتران التمويه»[1].

نخلص مما تقدم؛ إلى أن التوقيع الإلكتروني بصوره المستحدثة يمكنه أداء نفس الوظائف التي يشترطها القانون في التوقيع التقليدي، سواء من حيث تحديد هوية الشخص الموقع أو التعبير عن إرادة صاحب التوقيع، وكذلك ضمان سلامة المحرر. إلا أن هذه الصور المختلفة للتوقيع الإلكتروني تتفاوت فيما بينها على تحقيق هذه الوظائف، وبناء على هذا التفاوت بُنيت مستويات للاعتراف بها من قبل المشرعين، ومنح لكل منها حجية قانونية مناسبة لها في الإثبات.

= للتفصيل أكثر راجع: **منير محمد الجنبيهي، ممدوح محمد الجنبيهي،** التبادل الإلكتروني للبيانات، دار الفكر الجامعي، مصر، 2004، ص26.

)-1(CAPRIOLI .E-A, Sécurité et confiance dans le commerce électronique: signature numérique et autorité de certification ،J.C. P ed G,1998,p588.

مشار إليه لدى **بلقنيشي حبيب،** مرجع سابق، ص133.

المبحث الثاني
حجية التوقيع الإلكتروني في الإثبات

لم يعُد بإمكان التوقيع التقليدي الاستجابة لكافة المعاملات في وقتنا الراهن، خصوصا بعد انتشار المعاملات الإلكترونية التي تتم في بيئة افتراضية لا مادية، تقوم على مستندات ودعائم إلكترونية، ما فرض ظهور التوقيع الإلكتروني الذي يستجيب ويتناسب مع هذه البيئة الإلكترونية.

يحاكي التوقيع الإلكتروني التوقيع التقليدي في تحقيق وظائفه على الرغم من اختلاف بيئة كل منهما، إذ يعملان على تجسيد الثقة في التعاملات من خلال تحديد هوية المتعاملين، والتعبير عن إرادتهم بالالتزام بمضمون المعاملة الموقع عليها، وكذا ضمان سلامة ما تم التوقيع عليه من التعديل والتحريف.

بناء على هذه الوظائف أقرّت تشريعات الإثبات الإلكتروني بالحجية القانونية للتوقيع الإلكتروني في الإثبات، إلا أن هذا الإقرار لم يكن مطلقا بل قيدته بضرورة استيفاء التوقيع الإلكتروني للشروط والضوابط الفنية المحددة قانونا حتى يكتسب الحجية القانونية، بل والأكثر من ذلك فقد ميّزت بين الحجية الممنوحة للتوقيعات الإلكترونية المستوفية لكافة الشروط وجعلتها في مرتبة أعلى من الحجية الممنوحة للتوقيعات الإلكترونية التي لم تستوف كافة الشروط المقررة قانونا **(مطلب أول)**.

إلا أن منح التوقيع الإلكتروني لذات الحجية المقررة للتوقيع التقليدي من قبل بعض التشريعات بشكل عام دون تعرضها لبعض التفاصيل، أثار مسألة في غاية الأهمية ألا وهي حالة التنازع فيما بين الأدلة الكتابة؛ أي حالة التعارض بين مضمون محرر ورقي وآخر إلكتروني، مما يدفع بالقاضي إلى الترجيح بين الدليلين بناء على مدى استيفاء صور التوقيع الإلكتروني للشروط القانونية والفنية المحددة قانونا **(مطلب ثان)**.

المطلب الأول
شروط حجية التوقيع الإلكتروني في الإثبات

استنادا إلى ما سبق ذكره من تعريفات للتوقيع الإلكتروني، نجد أن معظم التشريعات الدولية منها أو الوطنية قد ميّزت بين التوقيع الإلكتروني البسيط والتوقيع الإلكتروني المتقدم أو المؤمن، حيث أنها منحت الحجية الكاملة للتوقيع الإلكتروني المتقدم مقارنة بالتوقيع الإلكتروني البسيط، غير أنها لم تُهدر قيمة هذا الأخير، إذ اعتبرته مقبولا في الإثبات مقارنة بالتوقيع الإلكتروني المتقدم الذي يعتبر موثوقا فيه إلى غاية إثبات العكس.

يجدر بنا القول أن هذه الموثوقية التي مُنحت للتوقيع الإلكتروني المتقدم متأتية من الشروط القانونية اللازمة لقيامه، وهي تكاد تكون متطابقة في معظم التشريعات، غير أن الاختلاف يبقى من حيث الصياغة القانونية للمواد فقط، وتتمثل هذه الشروط في كل من شرط تحديد هوية الموقع، شرط السيطرة الحصرية على وسائل إنشاء التوقيع الإلكتروني، إضافة إلى إمكانية كشف أي تعديل أو تغيير لاحق للبيانات المدرج عليها، مع ضرورة إنشاء التوقيع الإلكتروني بواسطة آلية إنشاء توقيع إلكتروني موصوفة، واعتماده على شهادة تصديق إلكتروني موصوفة.

عند استقراء الشروط السابقة يتضح لنا إمكانية تصنيفها إلى صنفين؛ الصنف الأول يتعلق بشروط شخصية لصحة التوقيع الإلكتروني ترتبط أساسا بشخص الموقع وإرادته **(فرع أول)**، والصنف الثاني عبارة عن شروط موضوعية لصحة التوقيع الإلكتروني تتعلق بالتوقيع في حد ذاته **(فرع ثان)**.

الفرع الأول
الشروط الشخصية لصحة التوقيع الإلكتروني

تتعلّق هذه الشروط أساسا بشخص الموقّع وإرادته؛ وتتمثّل في كل من شرط تحديد التوقيع الإلكتروني لهوية الموقع، وشرط ارتباطه به لوحده دون غيره، ومفاد هذين الشرطين أن ينسب

التوقيع إلى شخص معين بذاته، مع التأكد من رضاء صاحب التوقيع بمضمون التصرف القانوني الموقع عليه.

هذا وقد أقرت أغلب التشريعات الدولية والوطنية بهذين الشرطين، إلا أننا نجد من التشريعات من نصت عليهما في شرط واحد ومنها من فصلت بين الشرطين، إذ نص قانون اليونسترال النموذجي بشأن التوقيعات الإلكترونية لعام (2001)[1]، على هذا الشرط من خلال المادة (3/6) منه على أن: «**يعتبر التوقيع الإلكتروني قابلا للتعويل عليه لغرض الوفاء بالاشتراط المشار إليه في الفقرة 01 إذا:**

أ- **كانت بيانات انشاء التوقيع مرتبطة في السياق الذي تستخدم فيه بالموقع دون أي شخص آخر...**». حيث اشترط ارتباط بيانات إنشاء التوقيع بالموقع وليس ارتباط التوقيع بالموقع، فمن الأدق أن يشترط في التوقيع قدرته على تحديد هوية الموقع، وليس ارتباطه بالموقع.

في حين نجد التنظيم الأوروبي رقم (910-2014) المتعلق بتحديد الهوية الإلكترونية وخدمات الثقة في المعاملات الإلكترونية داخل السوق الداخلي سالف الذكر، أنه فصل بين الشرطين ونص على كل واحد منهما بشكل مستقل، ذلك من خلال نص المادة (26) منه حيث ورد فيها أن: «**التوقيع الإلكتروني المتقدم هو التوقيع الذي يفي بالمتطلبات التالية:**

1- أن يكون مرتبط بالموقع بصفة منفردة،

2- أن يحدد هوية الموقع...».

وقد تبنى المشرع الفرنسي نفس منهج التنظيم الأوروبي، حيث نص في المادة (1ف 2) من المرسوم (2017-1416) المتعلق بالتوقيع الإلكتروني سالف الذكر على أن: «**التوقيع الإلكتروني الموصوف هو التوقيع الإلكتروني المتقدم وفقا للمادة 26 من التنظيم الأوروبي...**».

---

(1)- قانون اليونسترال النموذجي بشأن التوقيعات الإلكترونية لعام (2001)، مرجع سابق.

بناء على ذلك؛ يكون المشرع الفرنسي قد اشترط ذات الشروط التي جاء بها التنظيم الأوروبي بخصوص التوقيع الإلكتروني المتقدم، والتي تتضمن شرط تحديد هوية الموقع وارتباطه به دون غيره.

كما سلك المشرع الأردني الاتجاه نفسه، حيث فصل بين الشرطين من خلال نص المادة (15) من قانون المعاملات الإلكترونية الأردني (15 لسنة 2015)[1]، والتي جاءت على النحو التالي: «**يعتبر التوقيع الإلكتروني محميا إذا توافرت فيه الشروط التالية مجتمعة:**

أ- إذا انفرد به صاحب التوقيع ليميزه عن غيره؛

ب- إذا كان يحدد هوية صاحب التوقيع...».

أما عن المشرع المغربي فقد عبر عن الشرطين بصيغة واحدة من خلال المادة (6 ف 1) من القانون (05-53)[2] المتعلق بالتبادل الإلكتروني للمعطيات القانونية على أن: «**يجب أن يستوفي التوقيع الإلكتروني المؤمن، المنصوص عليه في الفصل 417/3 من الظهير الشريف المعتبر بمثابة قانون الالتزامات والعقود الشروط التالية: أن يكون خاصا بالموقع...**».

كذلك الحال بالنسبة للمشرع المصري إذ نص من خلال المادة (18) من قانون التوقيع الإلكتروني (15 لسنة 2004)[3]، على أنه: «**يتمتع التوقيع الإلكتروني والكتابة الإلكترونية والمحررات الإلكترونية بالحجية في الإثبات إذا ما توافرت فيها الشروط الآتية:**

ارتباط التوقيع بالموقع وحده دون غيره...».

لم يكتف المشرع المصري بالنص على هذا الشرط فقط، بل بين من خلال المادة (9) من اللائحة التنفيذية لقانون التوقيع كيفية تحقق هذا الشرط من الناحية الفنية والتقنية، إذ تنص هذه المادة على أنه: «**يتحقق من الناحية الفنية والتقنية ارتباط التوقيع الإلكتروني بالموقع وحده**

(1)- قانون المعاملات الإلكترونية الأردني (15 لسنة 2015)، مرجع سابق.

(2)- القانون (05-53) المتعلق بالتبادل الإلكتروني للمعطيات القانونية المغربي، مرجع سابق.

(3)- قانون التوقيع الإلكتروني المصري (15 لسنة 2004)، مرجع سابق.

دون غيره متى استند هذا التوقيع إلى منظومة تكوين بيانات إنشاء توقيع إلكتروني مؤمنة على النحو الوارد في المواد (2-3-4) من هذه اللائحة، وتوافرت إحدى الحالتين الآتيتين:

أ- أن يكون هذا التوقيع مرتبط بشهادة تصديق إلكتروني معتمدة ونافذة المفعول صادرة من جهة تصديق إلكتروني مرخص لها أو معتمدة؛

ب- أن يتم التحقق من صحة التوقيع الإلكتروني طبقا للمادة 7 من هذه اللائحة»[1].

أما بالنسبة للمشرع الجزائري فنجده قد سلك نفس منهج التنظيم الأوروبي (910-2014) أين فصل بين الشرطين ونص على كل واحد منهما بشكل منفرد، ذلك من خلال المادة (7) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين، إذ ورد نصها كالآتي: «**التوقيع الإلكتروني الموصوف هو التوقيع الإلكتروني الذي تتوفر فيه المتطلبات الأتية:**

1-...

2- أن يرتبط بالموقع دون سواه،

3- أن يمكن من تحديد هوية الموقع...».

لكن وعلى عكس المشرع المصري، لم يبيّن المشرع الجزائري كيفية تحقق هذين الشرطين من الناحية القانونية الفنية والتقنية، الأمر الذي ينبغي على المشرع الجزائري التنبّه له مع ضرورة التدّخل التشريعي لسد هذا الفراغ، وفي ظل غياب أي نص يوضّح ذلك تبقى السلطة

---

(1) - تنص المادة (7) من اللائحة التنفيذية لقانون التوقيع المصري بأنه: «**تقدم الهيئة (هيئة تنمية صناعة تكنولوجيا المعلومات)، بناء على طلب كل ذي شأن، خدمة فحص التوقيع الإلكتروني نظير مقابل يحدد فئاته مجلس إدارة الهيئة، وتتحقق الهيئة في سبيل القيام بذلك مما يأتي:**

أ- سلامة شهادة التصديق الإلكتروني وتوافقها مع بيانات إنشاء التوقيع الإلكتروني،

ب- إمكان تحديد مضمون المحرر الإلكتروني الموقع بدقة».

التقديرية للقضاة للتأكّد من صحة هذين الشرطين مستعينين في ذلك بتقارير الخبراء والمختصين[1].

الفرع الثاني
الشروط الموضوعية لصحة التوقيع الإلكتروني

تتعلق هذه الشروط أساسا بشرط سيطرة الموقع الحصرية على وسائل إنشاء التوقيع الإلكتروني **(أولا)**، شرط كشف التوقيع الإلكتروني لأي تعديل أو تغيير لاحق للبيانات المدرج عليها **(ثانيا)**، شرط إنشاء التوقيع الإلكتروني بواسطة آلية إنشاء توقيع إلكتروني مؤمنة **(ثالثا)**، والشرط الأخير يتمثل في اعتماد التوقيع الإلكتروني على شهادة تصديق إلكتروني موصوفة **(رابعا)**، وسنتطرق فيما يلي لتوضيح كل شرط على حدى.

أولا: شرط سيطرة الموقع الحصرية على وسائل إنشاء التوقيع الإلكتروني

يتحقّق هذا الشرط إذا كان بإمكان الموّقع السيطرة على الوسيط الإلكتروني[2]، بحيث تكون أدوات ووسائل إنشاء التوقيع تحت سيطرته وحده، ومن هذه الوسائل على سبيل المثال لا الحصر؛ أجهزة تسجيل البصمات والمجسّات وأجهزة وأنظمة التشفير، شبكات الاتصالات التي تربط بين هذه الأدوات والأنظمة، هذا بالإضافة إلى البرامج المستحدثة في التشغيل وما في حكمها [3]. ولضمان هذه السيطرة لابد من بقاء منظومة إحداث ذلك التوقيع سرا لا يطلع عليها

---

(1) - تنص المادة 126 من القانون 08-09 المتضمن قانون الإجراءات المدنية والإدارية مؤرخ في 18 صفر عام 1429 موافق 25 فيفري 2008، ج ر ع 21 صادر بتاريخ 23 أفريل 2008: «**يجوز للقاضي من تلقاء نفسه أو بطلب أحد الخصوم تتعين خبير أو عدة خبراء من نفس التخصص أو من تخصصات مختلف**».

(2)- الوسيط الإلكتروني: هو آلية إنشاء التوقيع الإلكتروني، وقد عرفها المشرع الجزائري بنص المادة (2 ف 4) من القانون (15-04) بأنها: «... **جهاز أو برنامج معلوماتي معد لتطبيق بيانات إنشاء التوقيع الإلكتروني**».

(3)- **علي أبو مارية**، التوقيع الإلكتروني ومدى قوته في الإثبات، دراسة مقارنة، مجلة جامعة التحليل للبحوث، المجلد05، العدد 02، فلسطين 2010،، ص 119.

أحد حتى لا يساء استعماله من قبل الغير، سيما وأن التوقيع تترتب عليه آثار قانونية في حق الموقّع وحق الغير[1].

أما إذا فقد الموقّع سيطرته على الوسيط الإلكتروني وأصبحت بيانات إنشاء التوقيع الإلكتروني غير سرية، بحيث يعلمها أشخاص آخرون غير الموقّع، فإن التوقيع الإلكتروني لا يعتبر حجة في الإثبات، لأن تمييز هوية الموقّع وتحديد شخصيته بالرجوع إلى هذا التوقيع يكون أمرا مشكوكا فيه.

والمقصود ببيانات إنشاء التوقيع الإلكتروني، في سياق التوقيعات الإلكترونية التي ليست توقيعات رقمية، هو الإشارة إلى المفاتيح السرية أو الرموز أو العناصر الأخرى التي تستخدم في عملية إنشاء التوقيع الإلكتروني. فبالنسبة للتوقيعات الإلكترونية التي تعتمد على الخواص الحيوية للموقع، فمثلا يكون العنصر الأساسي هو مؤشر القياس الإحيائي مثل بصمة الإصبع أو بيانات فحص الشبكية، ولا يشمل التعريف سوى العناصر الجوهرية التي ينبغي الحفاظ على سريتها لضمان نوعية عملية التوقيع[2].

أما بالنسبة للتوقيعات الرقمية التي تعتمد على الترميز غير المتناظر؛ فإن العنصر التشغيلي الجوهري المرتبط الذي يمكن وصفه بأنه مرتبط بالموقّع، هو زوج مفاتيح الترميز (مفتاح التشفير الخاص ومفتاح التشفير العام)، إلا أن وصف بيانات إنشاء التوقيع في هذه الحالة لا يشمل سوى مفتاح التشفير الخاص[3].

---

(1)– **محمد رضا أزرو**، مرجع سابق، ص 203.

(2)– **أمين فرج يوسف**، التوقيع الإلكتروني، دار المطبوعات الجامعية، مصر، 2008. ص80.

(3) – **باطلي غنية**، فعالية التوقيع الإلكتروني في توثيق البيانات والكتابة الإلكترونية، مجلة الأبحاث القانونية والسياسية، جامعة سطيف، – العدد 02، مارس، 2020، ص 103؛ أنظر أيضا: **إكرام رقيعي**، خصوصية التوقيع الإلكتروني في العقد التجاري الإلكتروني على ضوء القانون رقم 18–05، مجلة العلوم القانونية والسياسية، جامعة الوادي، المجلد 10، العدد 02، سبتمبر 2019، ص 1677.

نجد أن هذا الشرط قد أورده قانون اليونسترال بشأن التوقيعات الإلكتروني لعام (2001) من خلال المادة(3/6/ب)[1]، كما أورده التنظيم الأوروبي (910-2014) من خلال المادة (26) سالفة الذكر[2]، ونص عليها المشرع الفرنسي من خلال المادة (1)[3] من المرسوم التنفيذي (2017-1416)، كما نص عليها المشرع المصري من خلال المادة (18 ف 2)[4]من القانون (15 لسنة 2004)، ونص عليها المشرع المغربي من خلال المادة (6 فـ2)[5] من القانون (05-53)، في حين نجد أن المشرع الجزائري كان قد تطرق إليها من خلال المرسوم التنفيذي رقم (07-162) وذلك في المادة (3 مكرر) منه[6] ، وقد نص على هذا الشرط أيضا في المادة (7 ف 5) من القانون (15-04):«... **أن يكون منشأ بواسطة وسائل تكون تحت التحكم الحصري للموقع** ».

غير أننا نجد أن المشرع المصري هو الوحيد الذي بيّن كيفية تحقّق شرط سيطرة الموقع وحده دون غيره على وسائل إنشاء التوقيع الإلكتروني، إذ نص بموجب المادة (10) من

---

(1)- تنص المادة (3/6/ب) من قانون اليونسترال بشأن التوقيعات الإلكتروني لعام (2001) على أن: «**تكون بيانات إنشاء التوقيع الإلكتروني خاضعة وقت التوقيع لسيطرة الموقع دون أي شخص آخر**».

)-2(Article26: «**Une signature électronique avancée satisfait aux exigences suivantes:...**
c) avoir été créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif… »
)-3(- Art. 1er. – **La fiabilité d'un procédé de signature électronique est présumée, jusqu'à preuve du Contraire, lorsque ce procédé met en œuvre une signature électronique qualifiée. Est une signature électronique qualifiée une signature électronique avancée, conforme à l'article 26 du règlement susvisé et créée à l'aide d'un dispositif de création de signature électronique qualifié répondant aux exigences de l'article 29 dudit règlement, qui repose sur un certificat qualifié de signature électronique répondant aux exigences de l'article 28 de ce règlement.**

(4)- تنص المادة (18 فـ2) من القانون (15 لسنة 2004) على أن: «**يتمتع التوقيع الإلكتروني والكتابة الإلكترونية والمحررات الإلكترونية بالحجية في الإثبات إذا ما توافرت فيه الشروط الآتية: …**

ب- سيطرة الموقع وحده دون غيره على الوسيط الإلكتروني»

(5)- تنص المادة (6 ف 2) من القانون (05-53) المتعلق بالتبادل الإلكتروني للمعطيات القانونية على أن: «**يجب أن يستوفي التوقيع الإلكتروني المؤمن، المنصوص عليه في الفصل 417/3 من الظهير الشريف المعتبر بمثابة قانون الالتزامات والعقود الشروط التالية: … أن يتم إنشاءه بوسائل يمكن للموقع الاحتفاظ بها تحت مراقبته الخاصة بصفة حصرية…**».

(6)- تنص المادة (3) مكرر من المرسوم التنفيذي رقم (07-162) على أن: «**التوقيع الإلكتروني المؤمن هو توقيع يفي بالمتطلبات الآتية: …**

يتم إنشاؤه بوسائل يمكن أن يحتفظ بها الموقع تحت رقابته الحصرية…»

اللائحة التنفيذية لقانون التوقيع الإلكتروني على أن: «**تتحقق من الناحية الفنية والتقنية، سيطرة الموقع وحده دون غيره، على الوسيط الإلكتروني المستخدم في عملية تثبيت التوقيع الإلكتروني عن طريق حيازة الموقع لأداة حفظ المفتاح الشفري الخاص، متضمنة البطاقة الذكية المؤمنة والكود السري المقترن بها**».

مما تقدم؛ نتساءل حول مدى إمكانية إنابة الموقّع لشخص آخر باستعمال بيانات إنشاء التوقيع الإلكتروني باسمه أو السماح له باستعمال مفتاح التشفير الخاص أو البطاقة الذكية الخاصة به؟

يعتبر بعض الفقه بأن نصوص قواعد الإثبات الخاصة بالتوقيع الإلكتروني جاءت صريحة وواضحة في اشتراط ضرورة السيطرة الحصرية للموقع وحده دون غيره على بيانات إنشاء التوقيع الإلكتروني. وعليه؛ فلا يجوز بأي حال من الأحوال قيام الشخص بإنابة غيره في التوقيع الإلكتروني في ظل النصوص الحالية، بل يجب أن تكون سيطرة الموقّع على منظومة إنشاء التوقيع الإلكتروني سيطرة كاملة وحصرية[1].

ما يؤكد هذا الرأي أيضا إلزام تشريعات الإثبات الإلكتروني مقدّم خدمات التصديق الإلكتروني بعدم حفظ أو نسخ العناصر الخاصة بالموقّع مثل مفاتيح التشفير الخاصة المستخدمة من طرفه لإنشاء توقيعه الإلكتروني، إذ نص المشرع الجزائري على ذلك من خلال نص المادة (48) من القانون (15-04) المتعلّق بالتوقيع والتصديق الإلكترونيين، حيث ورد نصها كالآتي: «**لا يمكن لمؤدي خدمات التصديق الإلكتروني حفظ أو نسخ بيانات إنشاء التوقيع الإلكتروني الذي منحت له شهادة التصديق الإلكتروني الموصوفة**». في حين نص عليها المشرع المصري بموجب المادة (12) من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري والتي تنص على أن:« **يجب أن يتوافر لدى طالب الحصول على الترخيص بإصدار شهادات التصديق الإلكتروني المتطلبات التالية:... ز- نظام حفظ بيانات إنشاء التوقيع الإلكتروني وشهادات التصديق الإلكتروني طوال المدة التي تحددها الهيئة في الترخيص، وتبعا لنوع الشهادة المصدرة وذلك فيما عدا مفاتيح الشفرة الخاصة التي تصدرها للموقع فلا**

(1)- **تامر محمد سليمان الدمياطي**، مرجع سابق، ص 602.

يتم حفظها إلا بناء على طلب من الموقع وبموجب عقد مستقل يتم إبرامه بين المرخص له والموقع وفقا للقواعد الفنية والتقنية لحفظ هذه المفاتيح التي يضعها مجلس إدارة الهيئة».

وفي حال ما إذا شـــك الموقّع أو فقد السيطرة على أدوات إنشاء توقيــعه الإلكتروني أو في حالة ما إذا أصبحت هذه البيانات غير مطابقة للمعلومات المتضمنة في شهادة التصديق؛ له أن يطلب إلغائها من طرف مؤدي خدمات التصديق الإلكتروني وفقا لنص المادة (61 ف 2)[1] من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين.

كما أكد القضاء الفرنسي على شرط سيطرة الموقع وحده دون غيره على وسائل إنشاء التوقيع الإلكتروني وإلا حال ذلك دون حجيته في الإثبات، من خلال حكم عن محكمة النقض الفرنسية بتاريخ (03 أفريل 2003)، والذي أيد حكم محكمة الاستئناف "Besançon" الصادر بتاريخ (20 أكتوبر 2000)، حيث اعتبرت فيه أن عريضة الاستئناف الموقعة إلكترونيا من طرف المحامي باستخدام الماسح الضوئي بالإضافة لاستخدام البيانات السرية له والتي من المفترض أن يكون هو الوحيد الذي يعلم بها. غير أن وقائع القضية تشير إلى وجود أشخاص آخرين يعملون بالمكتب كانوا على اطلاع بهذه البيانات، السبب الذي أدى بالمحكمة إلى الحكم بعدم صحة التوقيع الإلكتروني لعدم سيطرة الموقع الحصرية على وسائل إنشائه[2].

ثانيا: شرط كشف التوقيع الإلكتروني لأي تعديل أو تغيير لاحق للبيانات المدرج عليها

يقصد بهذا الشرط أن يكون التوقيع الإلكتروني مرتبطا ارتباطا وثيقا بالمستند الإلكتروني مما يدل على هوية صاحبه وإثبات قبوله بمضمون التصرف، وأن يكون محفوظا بطريقة تمكّن من الرجوع إليه عند الحاجة أو عند نشوء أي نزاع بخصوصه أو بين أطرافـــه، أي بطريقة تضمن ديمومته واستمراريته وإمكانية استرجاعه بطريقة آمنة [3].

---

(1)- تنص المادة 61 فقرة 02 من القانون 15-04: «... **وفي حالة الشك في الحفاظ على سرية بيانات إنشاء التوقيع، أو في حالة ما إذا أصبحت هذه البيانات غير مطابقة للمعلومات المتضمنة في شهادة التــصديق الإلكتروني، فإنه يجب على صاحب الشهادة أن يعمل على إلغائها من طرف مؤدي خدمات التصديق الإلكتروني...**».

)-2(.CA Besancon, Ch. Soc., 20 oct.2000,. Confirmé par Cass, Chambre civile 2, du 30 avril 2003.

(3)- فاطمة الزهراء تبوب، التوقيع والتصديق الإلكترونيين في ظل القانون رقم 15-04 المؤرخ في أول فبراير 2015، حوليات جامعة الجزائر، العدد 01، الجزء 02، ص 316.

وقد نص على هذا الشرط قانون اليونسترال بشأن التوقيعات الإلكترونية لعام (2001)[1] من خلال المادة(3/6/ج) على أن: «... **كان أي تغيير في التوقيع الإلكتروني، يُجرى بعد حدوث التوقيع قابلا للإكتشاف...**» كما أورده التنظيم الأوروبي (910-2014) من خلال المادة (26) سالفة الذكر، ونص عليها المشرع الفرنسي من خلال المادة (1)، سالفة الذكر من المرسوم التنفيذي (2017-1416).

بينما نص عليها المشرع الأردني من خلال المادة (15 ف 4) من القانون (15 لسنة 2015)، على أنه: «**يعتبر التوقيع الإلكتروني محميا إذا توافرت فيه الشروط التالية مجتمعة:... د- إذا ارتبط السجل الإلكتروني بصورة لا تسمح بإجراء تعديل على ذلك السجل الإلكتروني بعد توقيعه دون إحداث تغيير على ذلك التوقيع**».

في حين نص عليها المشرع المغربي من خلال المادة (6 ف3) من القانون (05-53) المتعلق بالتبادل الإلكتروني للمعطيات القانونية[2]، على أن: «: «**يجب أن يستوفي التوقيع الإلكتروني المؤمن، المنصوص عليه في الفصل 417/3 من الظهير الشريف المعتبر بمثابة قانون الالتزامات والعقود الشروط التالية: ... أن يضمن وجود ارتباط بالوثيقة المتصلة به بكيفية تؤدي إلى كشف أي تغيير لاحق أدخل عليها...**».

أما عن المشرع الجزائري فقد نص على هذا الشرط من خلال المادة (7 ف 6) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين على أن: «**التوقيع الإلكتروني الموصوف هو التوقيع الإلكتروني الذي تتوفر فيه المتطلبات الآتية _ أن يكون مرتبطا بالبيانات الخاصة به، بحيث يمكن الكشف عن التغييرات اللاحقة بهذه البيانات**».

نلاحظ من خلال هذه المادة أن المشرع الجزائري لم ينص صراحة على كيفية إمكانية كشف أي تعديل أو تبديل في بيانات المحرر الإلكتروني الموقع إلكترونيا من الناحية الفنية والتقنية. في حين نجد أن المشرع المصري نص على هذا الشرط في المادة 18 من قانون

(1)- قانون اليونسترال بشأن التوقيعات الإلكترونية لعام (2001)، مرجع سابق.

(2)- القانون (05-53) المتعلق بالتبادل الإلكتروني للمعطيات القانونية المغربي، مرجع سابق.

التوقيع الالكتروني: «**يتمتع التوقيع الإلكتروني والكتابة الإلكترونية والمحررات الإلكترونية بالحجية في الإثبات إذا ما توافرت فيه الشرط التالي: إمكانية كشف أي تعديل أو تبديل في بيانات المحرر الالكتروني أو التوقيع الالكتروني**».

بينما تنص المادة (11) من اللائحة التنفيذية لذات القانون: «**يتم من الناحية التقنية والفنية كشف أي تعديل أو تبديل في بيانات المحرر الإلكتروني الموقع إلكترونيا باستخدام تقنية شفرة المفتاحين العام والخاص، وبمضاهاة شهادة التصديق الإلكتروني بأصل هذه الشهادة وتلك البيانات أو بأي وسيلة مشابهة**».

نص المشرع المصري كذلك ومن خلال المادة (11) من اللائحة التنفيذية لقانون التوقيع الإلكتروني، على أهمية شهادة التصديق الإلكتروني التي يصدرها مقدمي خدمات التصديق الإلكتروني، إذ تعمل على التحقّق من صحة التوقيع الإلكتروني وتأكيد سلامة البيانات الموقع عليها من أي تعديل بالحذف أو الإضافة، حيث يتم مطابقة البيانات الجديدة بتلك المحتفظ بها لدى جهات التصديق التي قامت بإصدارها؛ ففي حال التطابق فهو تأكيد على سلامة التوقيع الإلكتروني والبيانات المدرجة عليه، أما في حال ظهور اختلاف بينهما فهذا يعني حصول تغيير أو تعديل في البيانات المدرج عليها التوقيع الإلكتروني[1].

ثالثا: شرط إنشاء الوقيع الإلكتروني بواسطة آلية إنشاء توقيع إلكتروني مؤمنة

اتفقت جميع تشريعات الإثبات الإلكتروني التي اطلعنا عليها على أن من بين المتطلبات الأساسية التي يقوم عليها "توقيع إلكتروني مؤمن" هو إنشاءه بواسطة آلية إنشاء توقيع إلكتروني تقوم على متطلبات قانونية وتقنية محددة، وعلى الرغم من إجماعهم على ضرورة وجود هذه الآلية إلا أنهم اختلفوا في تسميتها، فقد أطلق عليها التنظيم الأوروبي (910-2014) والمشرع الفرنسي بموجب المرسوم (2017-1416) مصطلح آلية إنشاء التوقيع الإلكتروني

(1)- باهة فاطمة، مرجع سابق، ص 193؛ راجع كذلك: **فضيلة يسعد**، القوة الثبوتية للتوقيع الإلكتروني في التشريع الجزائري، مجلة العلوم الإنسانية، المجلد 30، العدد 03، ديسمبر، 2019، ص 509.

الموصوفة[1]، في حين سمّاها المشرع الجزائري بآلية انشاء التوقيع الإلكتروني المؤمنة[2]، بينما فضّل المشرع المصري بإطلاق مصطلح منظومة إنشاء التوقيع الإلكتروني[3].

عرفّ المشرع الجزائري آلية إنشاء التوقيع الإلكتروني من خلال المادة (2 ف 4) من القانون (15-04) المتعلّق بالتوقيع والتصديق الإلكترونيين بأنها:« **جهاز أو برنامج معلوماتي معد لتطبيق بيانات إنشاء التوقيع الإلكتروني**»، وهو التعريف نفسه الي جاء به التنظيم الأوروبي (910-2014) من خلال المادة (3 ف 22): «**برنامج معلوماتي أو جهاز موضوع يهدف لإنشاء توقيع إلكتروني**»[4]، أما عن المشرع المصري فقد عرفها من خلال المادة (1 ف 18) من اللائحة التنفيذية لقانون التوقيع الإلكتروني بأنها: « **مجموعة عناصر مترابطة ومتكاملة، تحتوي على وسائط إلكترونية وبرامج حاسب آلي ويتم بواسطتها التوقيع إلكترونيا على المحرر الإلكتروني وذلك باستخدام بيانات إنشاء التوقيع الإلكتروني وشهادة التصديق الإلكتروني، كما يتم بواسطتها وضع وتثبيت المحرر الموقع إلكترونيا على دعامة إلكترونية**».

وتكون آلية إنشاء التوقيع الإلكتروني مؤمنة إذا ما استوفت الشروط المنصوص عليها في تشريعات الإثبات الإلكتروني، فقد نص عليها التنظيم الأوروبي (910-2014) في الملحق رقم (II) [5]، ونص عليها المشرع الجزائري في المادة (11) والتي يمكن اعتبارها شروط تقنية للتوقيع الإلكتروني والتي ورد نصها كالآتي:

---

(1) – أنظر المادة (12/3) من التنظيم الأوروبي (910-2014).

(2) – أنظر المادة (11) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين.

(3) – أنظر المادة (1 ف 18) من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري.

)-4(Article3/22 du règlement 910-2014**: « Aux fins du présent règlement, on entend par: …**
22- dispositif de création de signature électronique », un dispositif logiciel ou matériel configuré servant à créer une signature électronique ;…»

(5) - ANNEXE II du règlement 910-2014 *:* EXIGENCES APPLICABLES AUX DISPOSITIFS DE CRÉATION DE SIGNATURE ÉLECTRONIQUE QUALIFIÉS

1. Les dispositifs de création de signature électronique qualifiés garantissent au moins, par des moyens techniques et des procédures appropriés, que :

a) la confidentialité des données de création de signature électronique utilisées pour créer la signature électronique est suffisamment assurée ; =

«الآلية المؤمنة لإنشاء التوقيع الإلكتروني هي آلية إنشاء توقيع إلكتروني تتوفر فيها المتطلبات الآتية:

1- يجب أن تضمن بواسطة الوسائل التقنية والإجراءات المناسبة، على الأقل، ما يأتي:

أ- أن لا يمكن عمليا مصادفة البيانات المستخدمة لإنشاء التوقيع الإلكتروني إلا مرة واحدة، وأن يتم ضمان سريتها بكل الوسائل التقنية المتوفرة وقت الاعتماد؛

ب- ألا يمكن إيجاد البيانات المستعملة لإنشاء التوقيع الإلكتروني عن طريق الاستنتاج وأن يكون هذا التوقيع محميا من أي تزوير عن طريق الوسائل التقنية المتوفرة وقت الاعتماد؛

=b) les données de création de signature électronique utilisées pour créer la signature électronique ne peuvent être pratiquement établies qu'une seule fois ;

c) l'on peut avoir l'assurance suffisante que les données de création de signature électronique utilisées pour créer la signature électronique ne peuvent être trouvées par déduction et que la signature électronique est protégée de manière fiable contre toute falsification par les moyens techniques actuellement disponibles ;

d) les données de création de signature électronique utilisées pour créer la signature électronique peuvent être protégées de manière fiable par le signataire légitime contre leur utilisation par d'autres.

2. Les dispositifs de création de signature électronique qualifiés ne modifient pas les données à signer et n'empêchent pas la présentation de ces données au signataire avant la signature.

3. La génération ou la gestion de données de création de signature électronique pour le compte du signataire peut être seulement confiée à un prestataire de services de confiance qualifié.

4. Sans préjudice du paragraphe 1, point d), un prestataire de services de confiance qualifié gérant des données de création de signature électronique pour le compte d'un signataire ne peut reproduire les données de création de signature électronique qu'à des fins de sauvegarde, sous réserve du respect des exigences suivantes : =

=a) le niveau de sécurité des ensembles de données reproduits doit être équivalent à celui des ensembles de données d'origine ;

b) le nombre d'ensembles de données reproduits n'excède pas le minimum nécessaire pour assurer la continuité du service.FR L 257/112 Journal officiel de l'Union Européenne 28.8.2014

راجع كذلك المادة 01 من المرسوم الفرنسي رقم 2017-1416، والمادة 02 من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري: «تكون **منظومة تكوين بيانات إنشاء التوقيع الإلكتروني مؤمنة متى استوفت ما يأتي:**

أ- الطابع المتفرد لبيانات إنشاء التوقيع الإلكتروني،

ب- سرية بيانات إنشاء التوقيع الإلكتروني،

ج- عدم قابلية الاستنتاج أو الاستنباط لبيانات إنشاء التوقيع الإلكتروني،

د- حماية التوقيع الإلكتروني من التزوير، أو التقليد، أو التحريف، أو الاصطناع أو غير ذلك من صور التلاعب، أو من إمكان إنشائه من غير الموقع،

هـ- عدم إحداث أي إتلاف بمحتوى أو مضمون المحرر الإلكتروني المراد توقيعه،

و- ألا تحول هذه المنظومة دون علم الموقع علما تاما بمضمون المحرر الإلكتروني قبل توقيعه له».

ج- أن تكون البيانات المستعملة لإنشاء التوقيع الإلكتروني محمية بصفة موثوقة من =طرف الموقع الشرعي من أي استعمال من قبل الآخرين؛

2- يجب أن لا تعدل البيانات محل التوقيع وأن لا تمنع أن تعرض هذه البيانات على الموقع قبل عملية التوقيع».

ركزّ المشرع الجزائري عند وضعه للشروط الخاصة بآلية إنشاء التوقيع الإلكتروني، على البيانات المستخدمة في إنشائه، فيجب ألا تصادف هذه البيانات إلا مرة واحدة؛ أي تفردها وعدم تشابهها لا من بعيد أو قريب مع بيانات إنشاء توقيع إلكتروني آخر؛ مع ضمان سريتها. وألا تستخرج هذه البيانات عن طريق الاستنتاج، مع حماية هذه البيانات بصفة موثوقة من كل محاولة للتزوير أو الاختراق. وأخيرا ألا تعدّل هذه البيانات، وأن تعرض على الموقع قبل التوقيع.

والعبرة من حماية هذه البيانات راجع لكونها أساس قيام التوقيع الإلكتروني، فلا يتصوّر صحة توقيع إلكتروني قائم على بيانات مزورة، أو مسربة، أو مكررة.

أما عن آلية التحقّق من التوقيع الإلكتروني فقد عرفها المشرع الجزائري بنص المادة (2 ف 6) من القانون (15-04) سالف الذكر بأنها: «... **جهاز أو برنامج معلوماتي معد لتطبيق بيانات التحقق من التوقيع الإلكتروني**». أما البيانات اللازمة للتحقّق من التوقيع الإلكتروني فقد عرفها بنص المادة (2 ف 5) من القانون (15-04) بأنها: «**رموز أو مفاتيح التشفير العمومية أو أي بيانات أخرى، مستعملة من أجل التحقق من التوقيع الإلكتروني**».

فالآلية هي برنامج أو تجهيزات معلوماتية معدة من أجل وضع بيانات التحقق من التوقيع الإلكتروني موضع التطبيق، وقد اشترط المشرع الجزائري في نص المادة 12[1] من القانون (15-04) الموثوقية كما اشترطها من قبل في آلية إنشاء التوقيع الإلكتروني.

يكمن الفرق بين بيانات إنشاء التوقيع الإلكتروني وبيانات التحقق منه، في أن الأولى تكون حصرية للموقّع وحده، في حين أن الثانية تكون متاحة لكل شخص ليستعملها للتحقّق من صحة توقيع الموقّع.

ينص المشرع الجزائري على جملة من المتطلبات ينبغي أن تتوافر في آلية التحقق نص عليها في المادة (13) من القانون (15-04) [2] ونلخصها فيما يلي:

- أن تتطابق بيانات إنشاء التوقيع الإلكتروني مع البيانات المعروضة عند عملية التحقق، مع إمكانية التحقّق من التوقيع الإلكتروني بصفة أكيدة؛ إضافة إلى كون مضمون البيانات الموقعة عند الاقتضاء، محدّدا بشكل أكيد عند التحقّق من التوقيع الإلكتروني.
- وجوب التحقّق من مصداقية شهادة التصديق الإلكتروني بصفة قاطعة.
- وجوب التحقّق من هوية الموقع بصفة قاطعة.

---

(1)- تنص المادة 12 ق 15-04 من قانون التوقيع والتصديق الإلكترونيين: «**يجب أن تكون آلية التحقق من التوقيع الإلكتروني الموصوف موثوقة**».

(2)- تنص المادة 13 ق 15-04 من قانون التوقيع والتصديق الإلكترونيين: «**الآلية الموثوقة للتحقق من التوقيع الإلكتروني تتوفر فيها المتطلبات الآتية:**

1- أن تتوافق البيانات المستعملة للتحقق من التوقيع الإلكتروني مع البيانات المعروضة عند التحقق من التوقيع الإلكتروني.

2- أن يتم التحقق من التوقيع الإلكتروني بصفة مؤكدة وأن تكون نتيجة هذا التحقق معروضة عرضا صحيحا.

3- أن يكون مضمون البيانات الموقعة، إذا اقتضى الأمر، محددا بصفة مؤكدة عند التحقق من التوقيع الإلكتروني.

4- أن يتم التحقق بصفة مؤكدة من موثوقية وصلاحية شهادة التصديق الالكتروني المطلوبة عند التحقق من التوقيع الإلكتروني.

5- أن يتم عرض نتيجة التحقق وهوية الموقع بطريقة واضحة وصحيحة».

رابعا: شرط اعتماد التوقيع الإلكتروني على شهادة تصديق إلكتروني موصوفة

شهادة التصديق الإلكتروني؛ هي الشهادة التي تصدرها جهات التصديق الإلكتروني المرخص لها من قبل الجهة المختصة في الدولة بممارسة نشاطها[1]، لتقر بموجبها بأن التوقيع الإلكتروني هو توقيع صحيح وينسب لصاحبه، ويكون مستوفيا لكافة الشروط والمعايير المطلوبة فيه باعتباره دليل إثبات يعّول عليه.

من هذا المنطلق؛ فإن الهدف من إصدار شهادة التصديق الإلكتروني والمخزن بها جميع المعلومات العائدة لشخص ما؛ هو تأكيدها لصحة التوقيع الإلكتروني وارتباطه بالموقع، وأنه صادر ممن نسب إليه ولم يشبه أي تزوير أو تقليد أو تحريـف أو اصطـناع أو غيرها من صور التلاعب. كما تؤكد الشهادة على أن البيانات الموقّع عليها صحيحة ولم يطرأ عليها أي تبديل أو تعديل؛ سواء بالحذف أو بالإضافة أو التغيير، فتصبح هذه البيانات موثقة ولا يمكن إنكارها[2].

يقصد بشهادة التصديق الإلكتروني وفقا لنص المادة (2–ب) من قانون اليونسترال النموذجي بشأن التوقيعات الإلكتروني لسنة (2001): «...**رسالة بيانات أو سجل آخر يؤكدان ارتباط الموقع ببيانات إنشاء التوقيع الإلكتروني**».

نهج المشرع المصري نفس تعريف قانون اليونسترال من خلال المادة (1–و) من القانون (15 لسنة 2004) بأنها: «**الشهادة التي تصدر من الجهة المرخص لها بالتصديق وتثبت الارتباط بين الموقع وبيانات إنشاء التوقيع**».

بينما عرفها المشرع الأردني في المادة (2 فـ12) من القانون (15 لسنة 2015) بأنها: «**شهادة التوثيق الإلكتروني: الشهادة الصادرة عن جهة التوثيق الإلكتروني لإثبات نسبة التوقيع الإلكتروني إلى شخص معين استنادا إلى إجراءات توثيق معتمدة**».

---

(1)– سيتم تفصيل هذه الجهات في الباب الثاني، الفصل الأول من هذه الأطروحة.

(2)– **يوسف أحمد النوافلة**، حجية المحررات الإلكترونية في الإثبات، مرجع سابق، ص 88.

في حين عرفها التنظيم الأوروبي (910-2014) من خلال المادة (3 ف14) منه بأنها: «**شهادة إلكترونية ترتبط ببيانات التحقق من التوقيع الإلكتروني لشخص طبيعي وتؤكد على الأقل اسمه الحقيقي أو اسمه المستعار**» [1]، ونجد أن المشرع الجزائري قد سلك مسار التنظيم الأوروبي في تعريفه لشهادة التصديق الإلكتروني، حيث تنص المادة (2 ف7) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين على أن:« **الشهادة الإلكترونية هي وثيقة في شكل إلكتروني تثبت الصلة بين معطيات التحقق من التوقيع الإلكتروني والموقع**».

تجدر الإشارة إلى أن تشريعات الإثبات الإلكتروني الحديثة اشترطت أن تكون شهادة التصديق الإلكتروني موصوفة – أي تستجيب لمتطلبات قانونية محددة–[2]، حتى يتمتع التوقيع الإلكتروني بالحجية القانونية التامة المساوية لحجية التوقيع التقليدي في الإثبات.

)-1(Article 3/14 du règlement n° 910/2014: **«Certificat de signature élèctronique», une attestation électronique qui associe les données de validation d'une signature électronique à une personne physique et confirme au moins le nom ou le pseudonyme de cette personne; …».**

(2) – عرف المشرع الجزائري شهادة التصديق الإلكتروني الموصوفة في المادة (15) من القانون (15-04) ضمن الباب الثالث المعنون بالتصديق الإلكتروني وخصص لها فصلا كاملا معنونا بـ "شهادة التصديق الإلكتروني الموصوفة بأنها:

«شهادة التصديق الإلكتروني الموصوفة هي شهادة تصديق إلكتروني تتوفر فيها المتطلبات الآتية:

1- أن تمنح من قبل طرف ثالث موثوق أو من قبل مؤدي خدمات تصديق إلكتروني، طبقا لسياسة التصديق الإلكتروني الموافق عليها».

2- أن تمنح للموقع دون سواه،

3- ويجب أن تتضمن على الخصوص:

أ) – إشارة تدل على أنه تم منح هذه الشهادة على أساس أنها شهادة تصديق إلكتروني موصوفة،

ب) – تحديد هوية الطرف الثالث الموثوق أو مؤدي خدمات التصديق الإلكتروني المرخص له المصدر لشهادة التصديق الإلكتروني وكذا البلد الذي يقيم فيه،

ج)- اسم الموقع أو الاسم المستعار الذي يسمح بتحديد هويته،

د) – إمكانية إدراج صفة خاصة للموقع عند الاقتضاء، وذلك حسب الغرض من استعمال شهادة التصديق الإلكتروني،

هـ) – بيانات تتعلق بالتحقق من التوقيع الإلكتروني، وتكون موافقة لبيانات إنشاء التوقيع الإلكتروني،

و)- الإشارة إلى بداية ونهاية مدة صلاحية شهادة التصديق الإلكتروني،

ز)- رمز تعريف شهادة التصديق الإلكتروني، =

ولكي تحصل هذه الأخيرة على هذه الصفة وجب احتواءها على مجموعة من البيانات الإلزامية تتمثل أساسا في ثلاثة أصناف من البيانات، الأولى: تشمل المعلومات الخاصة بمقدم خدمات التصديق، والثانية: هي المعلومات والبيانات المتعلقة بصاحب التوقيع، والثالثة: تشمل المعلومات الخاصة بالشهادة، والهدف من هذه البيانات هو الإشهاد بأن التوقيع الإلكتروني صحيح ويستوفي الشروط والضوابط القانونية المطلوبة.

تماشيا مع تم ذكره؛ يتمتع التوقيع الإلكتروني بالحجية الكاملة في الإثبات المساوية لحجية التوقيع التقليدي؛ إذا ما استوفى الشروط القانونية المحددة من قبل تشريعات الإثبات الإلكتروني

= ح) – التوقيع الإلكتروني الموصوف لمؤدي خدمات التصديق الإلكتروني أو للطرف الثالث الموثوق الذي يمنح شهادة التصديق الإلكتروني،

ط) – حدود استعمال شهادة التصديق الإلكتروني، عند الاقتضاء،

ي) – حدود قيمة المعاملات التي قد تستعمل من أجلها شهادة التصديق الإلكتروني، عند الاقتضاء.

ك) – الإشارة إلى الوثيقة التي تثبت تمثيل شخص طبيعي أو معنوي أخر، عند الاقتضاء».

في حين نص عليها التنظيم الأوروبي 910-2014 من خلال الملحق الأول كما يأتي:

ANNEXE I

EXIGENCES APPLICABLES AUX CERTIFICATS QUALIFIÉS DE SIGNATURE ÉLECTRONIQUE

Les certificats qualifiés de signature électronique contiennent:

a) une mention indiquant, au moins sous une forme adaptée au traitement automatisé, que le certificat a été délivré comme certificat qualifié de signature électronique;

b) un ensemble de données représentant sans ambiguïté le prestataire de services de confiance qualifié délivrant les certificats qualifiés, comprenant au moins l'État membre dans lequel ce prestataire est établi, et:

— pour une personne morale: le nom et, le cas échéant, le numéro d'immatriculation tels qu'ils figurent dans les registres officiels,

— pour une personne physique: le nom de la personne;

c) au moins le nom du signataire ou un pseudonyme; si un pseudonyme est utilisé, cela est clairement indiqué;

d) des données de validation de la signature électronique qui correspondent aux données de création de la signature électronique;

e) des précisions sur le début et la fin de la période de validité du certificat;

f) le code d'identité du certificat, qui doit être unique pour le prestataire de services de confiance qualifié;

g) la signature électronique avancée ou le cachet électronique avancé du prestataire de services de confiance qualifié délivrant le certificat;

h) l'endroit où peut être obtenu gratuitement le certificat sur lequel reposent la signature électronique avancée ou le cachet électronique avancé mentionnés au point g);

i) l'emplacement des services qui peuvent être utilisés pour connaître le statut de validité du certificat qualifié;

j) lorsque les données de création de la signature électronique associées aux données de validation de la signature électronique se trouvent dans un dispositif de création de signature électronique qualifié, une mention l'indiquant, au moins sous une forme adaptée au traitement automatisé.

السالف ذكرها، لكن يبقى التساؤل عن مصير صور التوقيع الإلكتروني غير المستوفية لشروط التوقيع الإلكتروني الموصوف، وهل تُنسب لها حجية قانونية في الإثبات؟

لم تنكر تشريعات الإثبات الإلكتروني حجية صور التوقيع الإلكتروني غير المستوفية لشروط الموثوقية المحددة قانونا، وإنما تركت تقدير حجية هذا النوع من التوقيعات وما يتوافر فيه من عناصر أمان لسلطة القاضي التقديرية في ضوء ظروف كل حالة.

إذ نجد قانون اليونسترال النموذجي بشأن التوقيعات الإلكترونية لسنة (2001) قد نص من خلال المادة (3) على أن: «**لا يُطبق أي من أحكام هذا القانون، باستثناء المادة 5، بما يُشكل استبعادا أو تقييدا أو حرمانا من مفعول قانوني لأي طريقة لإنشاء توقيع إلكتروني تفي بالاشتراطات المشار إليها في الفقرة 1 من المادة 6، أو تفي على أي نحو آخر بمقتضيات القانون المطبق**».

بينما تنص المادة (25) من التنظيم الأوروبي رقم (910-2014) على: «**الأثر القانوني ومقبولية التوقيع الإلكتروني كدليل إثبات أمام القضاء لا يمكن أن يتم رفضه لمجرد أن هذا التوقيع تم تقديمه في الشكل الإلكتروني، أو لمجرد أنه لم يستوف متطلبات التوقيع الإلكتروني الموصوف**» [1].

في ذات السياق نص المشرع الجزائري من خلال المادة (9) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين على: «**بغض النظر عن أحكام المادة 8 أعلاه، لا يمكن تجريد التوقيع الإلكتروني من فعاليته القانونية أو رفضه كدليل أمام القضاء بسبب:**

1- شكله الإلكتروني، أو،
2- أنه لا يعتمد على شهادة تصديق إلكتروني موصوفة، أو،
3- أنه لم يتم إنشاؤه بواسطة آلية مؤمنة لإنشاء التوقيع الإلكتروني».

)-1(Article 25 du règlement 910-2014 : « **L'effet juridique et la recevabilité d'une signature électronique comme preuve en justice ne peuvent être refusés au seul motif que cette signature se présente sous une forme électronique ou qu'elle ne satisfait pas aux exigences de la signature électronique qualifiée ».**

لا بُدّ في الأخير من التأكيد على أن الحجية المقررة لصور التوقيع الإلكتروني غير المستوفية لشروط الموثوقية المحددة قانونا، لا تتساوى مع الاعتراف القانوني المقرر للتوقيع الإلكتروني الموصوف؛ كون هذا الأخير مُثبت بقوة القانون؛ أي اكتسابه لقرينة قانونية تفيد بصحته، على خلاف التوقيع الإلكتروني غير المستوف لشروط الموثوقية؛ أي افتقاده لهذه القرينة القانونية، مما يوجب على من يتمسك به في الإثبات أن يُقدم الدليل على صحته.

المطلب الثاني

أثر تفاوت صور التوقيع الإلكتروني على حجية المحررات الإلكترونية

بيّنا سابقا أن التشريعات الحديثة المتعلقة بالإثبات الإلكتروني قد أجمعت على الاعتراف بالمحررات الإلكترونية واعتبارها من قبيل الأدلة الكتابية في الإثبات، كما كرست مبدأ التعادل الوظيفي بين المحررات الموقّعة إلكترونيا والمحررات الموقّعة تقليديا، إذا ما استوفت الشروط المحددة قانونا.

إن هذا الاعتراف وإن كان يبدو في ظاهره سهل التطبيق إذا ما توافرت الشروط القانونية والفنية والتقنية المحددة قانونا، إلا أن واقع الحال يشير إلى ظهور شكل جديد من أشكال التنازع بين الأدلة الكتابية، إذ يمكن لأحد الخصوم الاحتجاج بمحرر إلكتروني، في حين يحتج خصمه بعكس ذلك بواسطة محرر ورقي، ويكون مضمون المحررين متعارضين، أو أن يتضمن أحد المحررين بيانا يخالف ما ورد في المحرر الآخر، ففي هذه الحالة يقع على القاضي وفقا لسلطته التقديرية أن يرجح أحد المحررين على الآخر واعتماده كدليل إثبات **(فرع أول)**، معتمدا في هذا الترجيح على الدور المهم الذي تلعبه مستويات التوقيع الإلكتروني في تحديد المحرر الواجب اعتماده في فك النزاع **(فرع ثان)**.

الفرع الأول

دور القاضي في الترجيح بين الأدلة الكتابية المتعارضة

لم تكن مسألة الترجيح بين المحررات التقليدية موضوعا لأي نص قانوني، إذ أن التشريعات كانت تعتبر المحررات الرسمية أقوى الأدلة نظرا للضوابط والإجراءات المتبعة في

انشائها، لتليها فيما بعد المحررات العرفية. إلا أنه بعد ظهور المحررات الإلكترونية والاعتراف التشريعي بحجيتها في الإثبات ومساواتها بالمحررات التقليدية وفقا لمبـدأ التعـــادل الوظيفـــي، ظهرت إشكالية التعارض فيما بين المحررات التقليدية والإلكترونية؛ ويتجلى الأمر بوضوح في حالة ما إذا قُدّم أمام القضاء محرر إلكتروني وآخر ورقي، يتعلقان بذات التصرف القانوني ويثبتانه باختلاف مضمونهما، مع تبوئهما لذات المرتبة.

بالعودة للتشريعات محل الدراسة نلاحظ غياب شبه تام لتنظيم مثل هذا النوع من التنازع على الرغم من أهميته البالغة، واقتصرت قوانينها على إقرار مبدأ المساواة بين المحررات الإلكترونية والمحررات الورقية، ما عدا التشريعين الفرنسي والمغربي اللذان عالجا هذه مسألة حيث ألقيا على القضاة مهمة تسوية المنازعات بين المحررات الإلكترونية والمحـــررات الورقية، وذلك بتحديد الدليل الكتابي الأقرب إلى الاحتمال عن غيره من الأدلة الكتابية أيا كانت دعامته.

نص المشرع المغربي بموجب المادة (5) من القانون (05-53) المتعلق بالتبادل الإلكتروني للمعطيات القانونية والتي أضاف من خلالها فقرة إضافية للفصل (417) من ظهير الالتزامات والعقود على أنه: «**إذا لم يحدد القانون قواعد أخرى ولم تكن هناك اتفاقية صحيحة بين الأطراف، قامت المحكمة بالبت في المنازعات بالدليل الكتابي بجميع الوسائل وكيفما كانت الدعامة المستعملة**»، في حين نص المشرع الفرنسي بموجب المادة (1368) من القانون المدني الفرنسي على أنه: «**في غياب الأحكام والاتفاقات المخالفة، يسوي القاضي منازعات الاثبات بالكتابة مقررا بكل الوسائل السند الأكثر احتمالا**» [1].

يظهر جليا من خلال هاتين المادتين أن كلا من المشرع المغربي والمشرع الفرنسي منحا القاضي السلطة التقديرية في حال التعارض بين الأدلة الكتابية أيا كانت الدعامة، ذلك ما لم يوجد نص قانوني أو اتفاق صحيح بين الأطراف على خلافه، غير أن المشرع الفرنسي نص على ترجيح الدليل الكتابي الأقرب إلى الاحتمال عن غيره من الأدلة الكتابية، في حين لم

)-1(-Article 1368: «**A défaut de dispositions ou de conventions contraires, le juge règle les conflits de preuve par écrit en déterminant par tout moyen le titre le plus vraisemblable**» Modifié par Ordonnance n°2016-131 du 10 février 2016 - art. 4.

ينص المشرع المغربي صراحة على ضرورة ترجيح القاضي للدليل الأكثر احتمالا وقربا للحق المدعى به؛ وهذا ما يؤخذ عليه.

باستقراء المادة (1368) من القانون المدني الفرنسي، نلاحظ أنه يتعين على القاضي عند إعمال سلطته التقديرية في الترجيح بين المحررات الإلكترونية والمحررات الورقية المتعارضة أن يتقيد بضابطين؛ يتمثل الضابط الأول في عدم وجود قواعد قانونية أو اتفاقات إثبات مبرمة فيما بين الأطراف تقضي بخلاف ذلك، بأن تمنح الأولوية لمحرر على آخر.

وعليه متى وجد نص قانوني يعطي الأفضلية لمحرر على آخر؛ كما هو الحال بالنسبة للمحررات الرسمية والمحررات العرفية؛ إذ تعتبر المحررات الرسمية أقوى في الحجية من المحررات العرفية، فيلزم القاضي بالأخذ بما هو ثابت في المحررات الرسمية؛ سواء أكانت إلكترونية أو تقليدية، أو كأن يتطلب القانون الكتابة كشرط لصحة التصرف – شرط للانعقاد– ففي حال التعارض بين محرر تقليدي ومحرر إلكتروني، وجب على القاضي الأخذ بالمحرر المستوفي لشرط الشكلية متى تبين صحته [1].

وفي ذات الاتجاه، يجوز للمتعاقدين الاتفاق على إعطاء أولوية لأحد المحررين في حال التعارض؛ كأن يتفقا على جعل الإثبات بالمحرر الإلكتروني فقط واستبعاد المحرر الورقي، أو الاتفاق على عكس ذلك، أي الإثبات بالمحرر الورقي فقط دون المحرر الإلكتروني، فإن وجد مثل هذا الاتفاق يتعين على القاضي الالتزام بما ورد فيه.

أما الضابط الثاني الذي وجب أن يتقيد به القاضي أثناء قيامه بالترجيح بين الأدلة الكتابية، أن تكون المحررات المتعارضة متساوية من حيث اعتبارها أدلة إثبات كاملة؛ بمعنى أن تتوافر فيها المتطلبات القانونية اللازمة لإضفاء الحجية عليها، سواء بالنسبة للمحررات الإلكترونية أو التقليدية [2]، فإن وجد من بينها من لا يستوف بعض أو أحد هذه الشروط

)-1(**CAÏDI Stéphane**, La preuve et la conservation de l'écrit dans la société de l'information, op.cit, p 92.

(2)– تامر محمد سليمان الدمياطي، مرجع سابق، ص 835؛ أنظر أيضا **مراد طنجاوي**، مرجع سابق، ص 283؛ وكذلك **بلقنيشي حبيب**، مرجع سابق، ص 99.

القانونية لاعتباره دليل كامل في الإثبات؛ فلا مجال للترجيح بينه وبين باقي الأدلة المستوفية للشروط القانونية المحددة لاعتبارها كأدلة كاملة في الإثبات.

خلاصة القول، أنه حسنا ما فعل كل من المشرع الفرنسي والمغربي بمنح السلطة التقديرية للقاضي في حال التعارض بين محرر إلكتروني ومحرر تقليدي مضمونا، وتساويهما من حيث توافر شروط اعتبار كل منهما دليلا كتابيا كاملا، على عكس ما فعل المشرع الجزائري الذي لم يتعرض بالتنظيم لمسألة التنازع بين الأدلة الكتابية في الإثبات، مما يرّجح الكفة في كل مرة بالأخذ بالمحررات الورقية، خصوصا في ظل هيمنة الدعامة المادية، مع كل ما تتمتع به من ثقة واطمئنان لدى القضاة في ظل عدم إلمامهم بالقواعد التقنية المتعلقة بالمحررات والتوقيعات الإلكترونية، ما سيؤثر سلبا على الثقة التي يحاول المشرع الجزائري منحها للتعاملات التي تتم بطريقة إلكترونية.

الفرع الثاني

دور التوقيع الإلكتروني في الترجيح بين الأدلة الكتابية

حرصت التشريعات الحديثة أن تكون المحررات الإلكترونية على قدم المساواة مع المحررات الورقية من حيث قبولها كدليل كتابي واكتسابها حجية في الإثبات، غير أن هذه المساواة المطلقة ستؤدي بالضرورة إلى حدوث حالات تعارض فيما بين المحررات الإلكترونية والمحررات الورقية؛ كأن يتضمن أحدهما بيانا يخالف البيان الوارد في المحرر الضد، مما دفع المشرع الفرنسي والمغربي إلى منح القاضي سلطة تقديرية واسعة في ترجيح الدليل الكتابي الأقرب إلى الاحتمال.

غير أن كيفية الترجيح بين هذه الأدلة لم تُرصد لها معايير محدّدة، بل للقاضي واسع النظر في تقدير ظروف كل حالة معروضة عليه، إلا أن نوع التوقيع الإلكتروني –بسيط، موصوف– الممهور به المحرر الإلكتروني يعلب دورا مهما في عملية الترجيح التي يقوم بها القاضي، من خلال ما يمنحه للمحرر الإلكتروني من ضمانات تكفل الثقة فيه، وذلك على النحو التالي:

أولا: التعارض بين محرر عرفي إلكتروني موصوف ومحرر عرفي ورقي

بيّنا سابقا من خلال هذه الدراسة أن تشريعات الإثبات الإلكتروني أقرت بالمساواة بين التوقيع الإلكتروني المؤمن[1] –الموصوف– والتوقيع الخطي التقليدي. في حين أضفى المشرع الفرنسي قرينة على التوقيع الإلكتروني تفيد بموثوقيته بموجب المادة (1) من المرسوم رقم (1416–2017) المتعلق بالتوقيع الإلكتروني[2]، والتي تنص على أن: «**موثوقية وسيلة التوقيع الإلكتروني تكون مفترضة حتى يثبت العكس عندما تكون الوسيلة منفذة بتوقيع إلكتروني موصوف، والتوقيع الإلكتروني الموصوف هو التوقيع الإلكتروني المتقدم وفقا للمادة 26 من التنظيم الأوروبي المشار إليه سابقا، ويتم إنشاؤه بواسطة آلية إنشاء توقيع إلكتروني موصوفة تفي بمتطلبات المادة 29 من هذا التنظيم، ويستند إلى شهادة موصوفة للتوقيع الإلكتروني تستجيب لمتطلبات المادة 28 من هذا التنظيم**»[3].

وعليه إذا صدر توقيع إلكتروني وفقا للضوابط القانونية المحددة قانونا التي تتسم بدقة إجراءاتها، ويكون قائما على أساس شهادة تصديق إلكتروني موصوفة، تثبُت له قرينة الموثوقية ويُعتبر على قدر كبير ومستوى عال من الأمان تنسحب على المحرر الإلكتروني الممهور به هذا التوقيع، فيكتسب الموثوقية ذاتها المقررة للتوقيع الإلكتروني؛ وعليه يعفى صاحب المحرر الإلكتروني الممهور بتوقيع إلكتروني مؤمن –موصوف– من إثبات صحته، لينتقل عبء

---

(1)– تجدر الإشارة إلى أن تشريعات الإثبات الإلكتروني قد اختلفت في تسمية التوقيع الإلكتروني المستوفي لكافة الشروط القانونية والفنية المحددة قانونا، والذي يوازي في حجيته حجية التوقيع الخطي التقليدي، فمنها من أطلق عليه مصطلح التوقيع الإلكتروني المتقدم كالتنظيم الأوروبي، وهناك من سماه بالتوقيع الإلكتروني المؤمن مثل التشريع المغربي، في حين سماه المشرع الأردني بالتوقيع الإلكتروني المحمي، أما عن المشرع الجزائري والفرنسي فقد أطلقا مصطلح التوقيع الإلكتروني الموصوف، بينما فضل المشرع المصري عدم إطلاق أي مسمى عليه واكتفى فقط بتحديد وضبط شروطه.

)-2(Décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique, JORF n°0229 du 30 septembre 2017 texte n° 8. Cité par : https://www.legifrance.gouv.fr/

)-3(Article 1 décret n° 2017-1416 **:«La fiabilité d'un procédé de signature électronique est présumée, jusqu'à preuve du contraire, lorsque ce procédé met en œuvre une signature électronique qualifiée. Est une signature électronique qualifiée une signature électronique avancée, conforme à l'article 26 du règlement susvisé et créée à l'aide d'un dispositif de création de signature électronique qualifié répondant aux exigences de l'article 29 dudit règlement, qui repose sur un certificat qualifié de signature électronique répondant aux exigences de l'article 28 de ce règlement ».**

إثبات عكس ذلك على الخصم المدعي بعدم صحة المحرر الإلكتروني، وهذا عكس ما تقرره القواعد العامة في الإثبات[1].

من جانب آخر، نجد أن المحرر العرفي الورقي لا يتمتع بأي مظهر خارجي يقطع بصحة صدوره ممن وقعه، فيكفي لتهدر صحته مجرد إنكاره، ذلك أنه يحرر في غياب موظف عام أو ضابط عمومي مما ينفي عنه صفة الرسمية.

وعليه؛ حين الترجيح بين محرر عرفي إلكتروني مؤمّن ومحرر عرفي ورقي تُرجح الكفة للمحرر الإلكتروني المؤمّن نظرا للقدر العالي من الثقة والأمان اللذان يحققهما، غير أنه في حال تم الاعتراف بالمحرر العرفي الورقي أو عدم إنكاره ممن صدر منه، فإنه يحوز على الحجية الكاملة في الإثبات توازي حجية المحرر الإلكتروني المؤمن، وفي هذه الحالة يقع عاتق القاضي مهمة الترجيح فيما بينهما بناء على ما يظهر له من أدلة الدعوى[2].

ثانيا: التعارض بين محرر عرفي إلكتروني بسيط ومحرر عرفي ورقي

التوقيع الإلكتروني البسيط هو التوقيع الذي لا تتوافر فيه الشروط القانونية والضوابط الفنية لاعتباره توقيعا إلكترونيا موصوفا، ومن ثَّم عدم مساواته بالتوقيع اليدوي الخطي، وفقا لما نصت عليه تشريعات الإثبات الإلكتروني ومن بينها المشرع الجزائري[3]، الذي اعتبر أن التوقيع الإلكتروني الموصوف هو وحده الموازي للتوقيع المكتوب.

---

(1)- تنص القواعد العامة في الإثبات أن المحرر العرفي يعتبر حجة على من صدر منه، متى اعترف به ولم ينكره صراحة، فإن اعترف صاحب التوقيع بصدور المحرر منه، اعتبر التوقيع توقيعه، ويصبح المحرر العرفي من حيث صدوره ممن وقعه بقوة المحرر الرسمي، ولا يجوز لصاحب التوقيع أن يعود بعد ذلك للإنكار، إلا أن يطعن بالتزوير.
أما إذا أنكر صاحب التوقيع صراحة توقيعه على المحرر العرفي، فإن المحرر يفقد قيمته مؤقتا، ويقع على المحتج بالمحرر عبئ إثبات صدوره من صاحب التوقيع. لمزيد من التفصيل راجع: **محمد حزيط**، مرجع سابق، ص94.

(2)- **تامر محمد سليمان الدمياطي**، مرجع سابق، ص 838.

(3)- تنص المادة (8) من القانون (15-04) على أنه: «**يعتبر التوقيع الإلكتروني الموصوف وحده مماثلا للتوقيع المكتوب، سواء لشخص طبيعي أو معنوي**».

وعليه، يعتبر المحرر الإلكتروني الممهور بتوقيع إلكتروني بسيط أقل قيمة من المحرر الإلكتروني الموصوف؛ وبالتالي أقل قيمة في حجيته من المحرر العرفي التقليدي، ذلك أنه من شروط اكتساب المحرر الإلكتروني لحجية في الإثبات تُعادل حجية المحرر التقليدي، وجوب مهره بتوقيع إلكتروني موصوف يستوفي الضوابط الفنية والتقنية والقانونية المحددة له؛ كأن ينشأ بواسطة آلية موصوفة لإنشاء التوقيع الإلكتروني، وأن يتم التحقق منه بناء على شهادة تصديق إلكتروني موصوفة تستجيب لشروط فنية وتقنية معينة.

وبيّنا فيما سبق، أن تشريعات الإثبات الإلكتروني لم تتنكر للتوقيعات الإلكترونية التي لا تتوافر على الشروط القانونية والفنية لاعتبارها توقيعات إلكترونية موصوفة، إذ نصت على مبدأ عدم تجريد التوقيع الإلكتروني من حجيته القانونية مثل ما فعل المشرع الجزائري [1]، إلا أن هذا الاعتراف لا يعني أبدًا المساواة فيما بينها وبين التوقيعات اليدوية التقليدية، بل وجب على من يدعي بها إثبات صحتها.

ومع ذلك، هنالك من يرى[2] ونحن نوافقه الرأي، أن المحرر العرفي الإلكتروني البسيط يأخذ ذات المرتبة المقررة للمحرر العرفي التقليدي في الإثبات نظرا لاتفاقهما في ضعف الضمانات المقررة لكل منهما، فالمحرر العرفي التقليدي قائم على عدم إنكار التوقيع ممن نُسب إليه، ويقع على عاتق من يتمسك به أن يُثبت صحته، وهو الأمر ذاته بالنسبة للتوقيع الإلكتروني البسيط؛ إذ يقع على عاتق من يتمسك به إثباته؛ وعليه يتساوى كل من المحرر التقليدي العرفي والمحرر الإلكتروني البسيط في الحجية، ويقع على عاتق القاضي فض التنازع فيما بينهما على أساس أدلة الدعوى.

---

(1)- تنص المادة (9) من القانون (15-04) على أنه: «**بغض النظر عن أحكام المادة 8 أعلاه، لا يمكن تجريد التوقيع الإلكتروني من فعاليته القانونية أو رفضه كدليل أمام القضاء بسبب:**

1- شكله الإلكتروني، أو،

2- أنه لا يعتمد على شهادة تصديق إلكتروني موصوفة، أو،

3- أنه لم يتم إنشاؤه بواسطة آلية مؤمنة لإنشاء التوقيع الإلكتروني».

(2)- تامر محمد سليمان الدمياطي، مرجع سابق، ص 839.

ثالثا: التعارض بين محرر عرفي إلكتروني موصوف ومحرر رسمي ورقي

بينت القواعد العامة في الإثبات أنه متى اكتسب المحرر صفة الرسمية بتوافره على الشروط الثلاث المحددة قانونا[1]، كأن يتم تحريره من قبل موظف عام أو ضابط عمومي أو شخص مكلف بخدمة عامة، وكذا في حدود اختصاصه، وأن يراعي الأشكال القانونية في تحريره، صار لهذا المحرر ذاتية في الإثبات، فلا يُطلب ممن يحتج به أن يُثبت صحته، ولا يكون هناك حاجة للإقرار به، وإنما يقع على عاتق من ينكره أن يقيم الدليل على بطلانه، ولا يتم ذلك إلا عن طريق الطعن بالتزوير.

وبينا كذلك من خلال هذه الدراسة إلى أن المحرر الإلكتروني الممهور بتوقيع إلكتروني موصوف، يتمتع بقرينة قانونية مفادها صحة التوقيع وسلامة البيانات المدونة عليه، مما يترتب على ذلك إعفاء صاحب المحرر من عبء إثبات صحته وسلامته المادية، لينتقل عبء إثبات عكس ذلك على من ينكره.

استنادا إلى ما سبق ذكره، نكون أمام محررين متساويين من حيث مصداقية التوقيع وبناء على ذلك وجوب الترجيح بينهما في حال تعارضهما، غير أنه لو سلمنا جدلا بذلك سيؤدي هذا الأمر إلى الانتقاص من قيمة المحرر الرسمي العرفي والذي يحظى بضمانات هامة لا تتوافر في المحرر العرفي الإلكتروني الممهور بتوقيع إلكتروني موصوف؛ ذلك لتحريره من قبل موظف عام مما يضفي عليه صفة الرسمية لا يمكن الطعن فيها إلا بالتزوير؛ على عكس المحرر الإلكتروني الممهور بتوقيع إلكتروني موصوف والذي يمكن إثبات عكسه بكل الطرق الممكنة.

وعليه؛ نرى أن المحرر الرسمي الورقي يتفوق على المحرر العرفي الإلكتروني الممهور بتوقيع إلكتروني موصوف من حيث الضمانات المقررة لكل منهما، مما يدفعنا للقول كذلك بأن المحرر العرفي الإلكتروني الممهور بتوقيع إلكتروني موصوف يقع في مرتبة أدنى من المحررات الرسمية الإلكترونية أو الورقية وفي مرتبة أعلى من المحررات العرفية الورقية.

---

(1)- راجع في هذا نص المادة 324 من القانون المدني الجزائري.

رابعا: التعارض بين محرر رسمي إلكتروني ومحرر رسمي ورقي

تعرضنا من خلال هذه الدراسة إلى إمكانية إنشاء محرر رسمي إلكتروني يتم عن طريق موظف عمومي، يستوفي كل الشروط القانونية التي تكفل صحته وسلامته المادية، مع مهره بالتوقيع الإلكتروني الموصوف للموظف العام وكذا التوقيعات الإلكترونية المحددة لهوية الأطراف المتعاقدة، مما يكسب المحرر الإلكتروني حجية قوية في الإثبات لا يجوز دحضها إلى عن الطريق الطعن بالتزوير.

تماشيا مع ما تم ذكره، نجد أن هذه الحجية المقررة للمحررات الرسمية الإلكترونية هي ذاتها المقررة للمحررات الرسمية التقليدية، على أساس توافرهما على الشرط الأساسي الذي يضفي عليهما طابع الرسمية، ألا وهو تحريرهما من قبل موظف عمومي، وهذا ما اتفقت عليه تشريعات الإثبات الإلكتروني عندما أقرت بضرورة عدم التمييز بين المحررات الرسمية بنوعيها –التقليدية والإلكترونية– في حال ما استوفت كل منهما الشروط القانونية لصحتها.

وإن كان هنالك من يرى [1] بأن الضمانات الممنوحة للمحرر الرسمي الإلكتروني تفوق الضمانات الممنوحة للمحرر الرسمي التقليدي، ذلك أنها ضمانات مزدوجة تتمثل في حضور الموظف العمومي، إضافة إلى افتراض موثوقية التوقيع الإلكتروني الموصوف الخاص به، وهو ما لا يتوفر في المحررات الرسمية التقليدية إلا بصورة نسبية، وبناء عليه تفوق المحرر الرسمي الإلكتروني على نظيره التقليدي، مما يستدعي بالضرورة عند الترجيح بينهما تغليب كفة المحرر الرسمي الإلكتروني.

إلا أننا نرى بأنه لا مجال للمفاضلة بين المحررات الرسمية الإلكترونية والورقية، كون أن المشرع الفرنسي لم يشترط أن تكون توقيعات الأطراف الإلكترونية التي تمهر بها المحررات الإلكترونية موصوفة، بل يتم بأخذ صورة لتوقيعهم الخطي عن طريق الماسح

(1)– لمزيد من التوضيح راجع في ذلك **تامر محمد سليمان الدمياطي**، مرجع سابق، ص 840؛ وكذلك: **باهة فاطمة**، مرجع سابق، ص 221.

الضوئي[1]، وعليه فهي لا تتوافر على عنصر الموثوقية، وبهذا لا يمكن القول بتفوق المحرر الرسمي الإلكتروني على نظيره المحرر الرسمي التقليدي؛ وإنما يخضعان لمبدأ المساواة الذي أقرته كل تشريعات الإثبات الإلكتروني.

نصل في الأخير، إلى أن حالات التنازع بين الأدلة الكتابية أمر مفروغ منه نتيجة لمبدأ التكافؤ بين الدليلين الكتابيين الورقي والإلكتروني الذي أقرتـــه تشريعات الإثبات الإلكتـــروني، ومنها المشرع الجزائري. وعلى الرغم من إمكانية حدوث حالات التنازع التي بيّناها سابقا لم تتدخل معظم التشريعات الحديثة لأجل تنظيمها، ما عدا ما نص عليه المشرع الفرنسي والمغربي عند منحهما للقاضي سلطة تقديرية في الترجيح بين الأدلة الكتابية المتعارضة، ليعتمد هذا الأخير في عملية الترجيح على مستوى الثقة والأمان المقرران للتوقيع الإلكتروني الممهور به المحرر الإلكتروني، فكلما كان التوقيع الإلكتروني مستوفيا لجميع الشروط الفنية والتقنية المحددة قانونا كلما تمتع بضمانات موثوقية تفوق أحيانا من حيث الحجية تلك الممنوحة للتوقيع المكتوب، ونتيجة لذلك تغليب كفته عند الترجيح.

)-1(Art 17 du décret n° 71-941: «**L'acte doit être signé par le notaire au moyen d'un procédé de signature électronique sécurisée conforme aux exigences du décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique.**
Cette signature est apposée par le notaire dès l'acte établi, si besoin après réunion des annexes à l'acte.
Pour leur signature, les parties et les témoins doivent utiliser un procédé permettant l'apposition sur l'acte notarié, visible à l'écran, de l'image de leur signature manuscrite.
Lorsque l'acte doit contenir une mention manuscrite émanant d'une personne qui y concourt, le notaire énonce que la mention a été apposée dans le respect des conditions prévues au second alinéa de l'article 1108-1 du code civil ».

خلاصة الباب الأول

خلاصة الباب الأول

أدى التطور التقني الحاصل في مجال تكنولوجيا المعلومات والاتصالات إلى زعزعة عدة مفاهيم تقليدية كانت راسخة في الفكر القانوني، ولعل أهمها الدليل الكتابي –المحرر والتوقيع– الذي ظل لعقود طويلة مرتبطا ارتباطا وثيقا بالدعامة المادية الورقية، إلا أن التطور التقني الحاصل أدى إلى ظهور أنماط وأشكال متعددة يتم من خلالها إبرام التصرفات القانونية، تعتمد في الأساس على دعامة لا مادية افتراضية نتج عنها ظهور نوع مستحدث من الأدلة الكتابية يتماشى والطبيعة التقنية تمثّلت أساسا في المحرر والتوقيع الإلكتروني.

ونظرا لحتمية التعامل بهذا الوافد الجديد ولضمان استقرار المعاملات في ظل تغير المفاهيم التقليدية للمحرر والتوقيع سارعت العديد من المؤسسات الدولية والإقليمية والوطنية ومنها المشرع الجزائري، إلى الاعتراف القانوني بالمحررات والتوقيعات الإلكترونية في الإثبات وذلك إما عن طريق تعديل القواعد القانونية العامة المتعلقة بالإثبات، أو باستحداث نصوص قانونية خاصة، أين اعترفت من خلالها بالأدلة الكتابية الإلكترونية واعتبرتها امتداد للأدلة الكتابية التقليدية، لا يختلفان إلا من حيث الدعامة التي يقوم عليها كل منهما، وبذلك تكون قد اعتمدت مبدأ النظير الوظيفي فيما بين المحررات الإلكترونية الممهورة بتوقيع إلكتروني، والمحررات التقليدية الممهورة بتوقيع عادي.

ونتيجة لإقرار مبدأ التعادل الوظيفي فيما بين الأدلة الكتابية التقليدية والأدلة الكتابية الإلكترونية؛ منحت تشريعات الإثبات الإلكتروني المحررات والتوقيعات الإلكترونية الحجية ذاتها المقررة للمحررات والتوقيعات التقليدية إذا ما استوفت الشروط القانونية والفنية المحددة قانونا؛ غير أننا بيّنا فيما سبق بخصوص حجية المحررات الإلكترونية في الإثبات –العرفية والرسمية– عدم ملائمة تطبيق القواعد العامة التي تحكم المحررات التقليدية على المحررات الإلكترونية مما استدعى ضرورة تنظيمها بموجب نصوص خاصة تتناسب والطبيعة الإلكترونية لهذه المحررات.

أما بخصوص التوقيع الإلكتروني فقد انتهينا إلى أن التطوّر التكنولوجي قد حرر فكرة التوقيع من أشكاله التقليدية– الإمضاء، الختم والبصمة– ليتم التعويل فيما بعد على

الوظائف التي يؤديها التوقيع بغض النظر عن شكله، وهو الأمر الذي تبنته تشريعات الإثبات الإلكتروني والمشرع الجزائري كذلك حين اعتمدت في تعريفها للتوقيع الإلكتروني على النهج الوظيفي، أين ركزت على الوظائف التي يؤديها هذا الأخير من تحديد هوية الموقع والتعبير عن رضائه، وكذا سلامة ما تم التوقيع عليه ما نتج عنه ظهور العديد من صور التوقيع الإلكتروني، غير أن هذه الصور تختلف وتتباين من حيث الحجية القانونية المقررة لكل منها.

فإذا ما استوفى التوقيع الإلكتروني للشروط القانونية والفنية المحددة قانونا؛ كأن تكون وسيلة إنشائه مؤمنة تستجيب لمتطلبات فنية وتقنية محددة قانونا؛ وأن يكون التحقق منه يستند إلى شهادة إلكترونية موصوفة تستجيب هي الأخرى لشروط فنية وتقنية معينة، اعتبر التوقيع الإلكتروني موصوفا وهو وحده الموازي في الحجية للتوقيع التقليدي المكتوب، أما إذا لم يستوف التوقيع الإلكتروني للشروط السابق ذكرها فاعتبر توقيعا إلكترونيا بسيطا لا يحوز لذات الحجية المقررة للتوقيع الإلكتروني الموصوف، وبالتالي لا يحوز حجية التوقيع التقليدي المكتوب، إلا أنه رغم ذلك لم تجرد تشريعات الإثبات الإلكتروني التوقيع الإلكتروني البسيط من فعاليته القانونية، واعتبرت بأنه ينبغي تقدير حجيته بالقدر المناسب استنادا إلى مدى الثقة في وسيلة إنشائه وحفظه.

وجدير بالذكر في هذا المقام، أن نبيّن دور المشرع الجزائري في تنظيم الأدلة الكتابية، خصوصا في ظل تأخره الملحوظ في تنظيم هذه المعاملات مقارنة بالتشريعات المقارنة، فأول ما نص عليه المشرع الجزائري كان من خلال التعديل الذي أدخله على القانون المدني سنة (2005)، أين اعترف من خلال نص المادة (323 مكرر 1) بالكتابة في الشكل الإلكتروني واعتبرها كالكتابة على الورق، واعترف بالتوقيع الإلكتروني من خلال نص المادة (327) من القانون المدني الجزائري، وعليه فقد اعترف المشرع الجزائري بالمحررات الإلكترونية وأضفى عليها حجية الأوراق العرفية شريطة أن تحتوي على توقيع إلكتروني يمكن من خلاله تحديد هوية الموقع وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها، وبذلك يكون قد أخرج فئة المحررات الرسمية من هذا الاعتراف.

بعد ذلك أصدر المشرع الجزائري القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين، الذي يهدف إلى تحديد القواعد العامة التي تنظم مسألة قبول التوقيع الإلكتروني في الإثبات، وعلى الرغم من مرور (10) سنوات من أول تعديل تضمنه القانون المدني، لم يكن القانون (15-04) بالمستوى الذي يمكنه من وضع أرضية قانونية صلبة للمعاملات الإلكترونية، حيث لم يتم التطرق إلى العديد من المسائل الجوهرية في تنظيم المعاملات الإلكترونية وعلى رأسها المحررات الإلكترونية الرسمية، والتي أبقاها المشرع الجزائري خارج دائرة المعاملات الإلكترونية، كما لم يُتبِع إصدار القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين، بنصوص تنظيمية تدخله حيز التنفيذ، خصوصا وأن الجزائر حاليا تعتبر في مرحلة انتقالية من العالم الورقي إلى العالم الافتراضي وجب فيه سن ترسانة قانونية تنظم كل الإشكالات وتسد كل الثغرات التي يمكن أن يطرحها هذا الانتقال، ولها في هذا أن تستفيد من تشريعات الدول التي سبقتنا في ذلك وعلى الخصوص المشرع الفرنسي.

الباب الثاني

الحماية المقررة لأدلة الإثبات الإلكتروني

الباب الثاني
الحماية المقررة لأدلة الإثبات الإلكتروني

فرضت المحررات والتواقيع الإلكترونية نفسها في التعامل، وأصبحت واقعا لا يمكن إنكاره وانتشر استعمالها انتشارا واسعا، لتشمل جميع الأنشطة الإدارية، الإقتصادية، الإنتاجية، المالية والخدماتية، الأمر الذي صاحبه ظهور مفاهيم عديدة لأنماط التعامل الإلكتروني الحديث كالتجارة الإلكترونية، والإدارة الإلكترونية، والحكومة الإلكترونية، والدفع الإلكتروني والعمليات المصرفية الإلكترونية والتصرفات المدنية الأخرى سواء بإبرامها أو إنهائها عبر الوسائط الإلكترونية كعقود البيع والايجار بين أشخاص عاديين، والإقرار أو الوقف أو الوصية وغيرها.

إلا أن الانتقال من مرحلة المعاملات الورقية إلى المعاملات الإلكترونية فتح باب الجدل حول صحة هذه المعاملات ومدى حجيتها في الإثبات، ومستوى الأمان الذي تحققه خصوصا في ظل بيئة افتراضية تعتبر كشبكة مفتوحة للملأ، مما يجعل البيانات المتداولة أكثر عرضة لمخاطر الاختراق والاعتراض والتخريب والتعييب والتعديل، وغيرها من المخاطر التي يمكن أن تتعرض لها في هذه البيئة، ذلك أن هذه الاعتداءات قد تستهدف المعلومات المبرمجة التي لها قيمة في الاثبات، وهو ما يهدد الثقة والأمان التي يجب أن تكون عليه المعاملات الإلكترونية.

لذلك سعت تشريعات الإثبات الدولي ككل؛ سواء الدولية منها أو الوطنية؛ إلى سن قوانين خاصة تعنى بإضفاء الحماية القانونية لضمان أمن وسلامة المحررات والتواقيع الإلكترونية، ولم تقتصر هذه التشريعات على توفير الحماية التقليدية المتمثلة في الحماية الجزائية والمدنية في آن واحد، بل قد تعدت ذلك إلى توفير نوع آخر من الحماية القبلية أو الوقائية يطلق عليها الحماية التقنية أو الفنية **(فصل أول)**؛ أي كل ما يتعلق بالأمن المعلوماتي وجميع الوسائل الكفيلة بضمان أمن وسرية وصحة المعلومات المتداولة إلكترونيا.

وباعتبار أنه من المستحيل، توفير نظام أمني دقيق وفعال بسبب تشابك العلاقات فيما بين المتعاملين عبر شبكة الانترنت، وجب أن يكون هذا النظام الأمني مدعم بنظام قانوني

واضح المعالم، يتكفل بحماية تلك البيانات بتجريم الأعمال الماسة بها سواء بتعديل القوانين العامة أو بسن نصوص قانونية خاصة، بمعنى توفير حماية تقنية تدعمها حماية تشريعية جزائية **(فصل ثان)**.

يبقى انتشار التعامل بالمحررات والتواقيع الإلكترونية رهين مدى توفير الحماية القانونية سواء التقنية – حماية وقائية–، أو الجزائية –حماية بعدية – الكافية لإعطاء ضمانات تشجع المتعاملين على الولوج إلى العالم الافتراضي وهم مطمئنين على صحة تعاملاتهم وأمن معلوماتهم من أي احتيال أو تسريب أو اختراق.

الفصل الأول
الآليات التقنية لحماية أدلة الإثبات الإلكتروني

تتمتع المعاملات في صورتها التقليدية بالأمن والثقة القانونيين؛ من حيث وجود محرر ورقي مكتوب ليس من السهولة إنكاره أو تغيير مضمونه، ولكن الأمر يختلف فيما يتعلق بدرجة الثقة والأمان التي يتمتع بها المحرر الإلكتروني مما يفتح باب النقاش حول توفير البيئة القانونية المناسبة للتعاملات الإلكترونية الآمنة، ولا تتوفر هذه البيئة الآمنة للمحرر الإلكتروني إلا من خلال ضمان صحة المعلومات الواردة فيه، وتأكيد هوية أطرافه ونسبة توقيعاتهم الإلكترونية إليهم، مع ضمان سلامة البيانات المتداولة من كل تعديل أو تحريف.

من هذا المنطلق سعت تشريعات الإثبات الإلكتروني الدولية منها والوطنية إلى خلق حماية قانونية تقنية تعنى بأدلة الإثبات الإلكتروني، من أجل بث الثقة في المعاملات التي تتم عبر الوسائط الإلكترونية، وقد بيّنا من خلال دراستنا سابقا أن كل هذه التشريعات قد نصت على ضرورة استجماع أدلة الإثبات الإلكتروني –المحررات والتواقيع الإلكترونية– لاشتراطات تقنية وفنية على درجة عالية من التعقيد حتى تتمتع بالحجية القانونية ذاتها المقررة لأدلة الإثبات التقليدي –المحررات والتواقيع التقليدية–.

تتمثل الاشتراطات القانونية التقنية والفنية التي نصت عليها تشريعات الإثبات الإلكتروني في آليتين اثنتين لا تقل إحداهما أهمية عن الأخرى، تتمثل الآلية الأولى في "التصديق الإلكتروني" في حين تتمثل الثانية في " الحفظ الإلكتروني"، وهما عبارة عن تقنيتين متكاملتين تعملان على ضمان أمن وسلامة المحررات والتواقيع الإلكترونية، مما يمنحهما حجية في الإثبات تعادل حجية المحررات والتواقيع التقليدية **(مبحث أول)**.

ولأجل التجسيد الفعلي للدور المهم الذي تلعبه هاتين الآليتين في ضمان أمن وسلامة أدلة الإثبات الإلكتروني، استحدثت تشريعات الإثبات الإلكتروني هيئات خاصة محايدة أسندت إليها مهمة التصديق والحفظ الإلكترونيين، إذ تعمل هذه الهيئات والتي يصطلح عليها "بهيئات التصديق الإلكتروني" على لعب دور الوسيط المؤتمن الضامن للمعاملات الإلكترونية، ونظرا

للدور المهم الذي تقوم به هذه الهيئات تدخلت تشريعات الإثبات الإلكترونية؛ سواء الدولية منها أو الوطنية؛ لتنظيم نشاطها وذلك من خلال تحديد التزاماتها وكذا مسؤولياتها **(مبحث ثان)**.

المبحث الأول

دور الحفظ والتصديق الإلكترونيين في تأمين أدلة الإثبات الإلكتروني

تتعززّ المعاملات الإلكترونية بقدر ما تتمتع به من ثقة وأمان لدى المتعاملين عبر الوسائط الإلكترونية، لذا يتطلب هذا النوع من التعاملات توفير الضمانات الكفيلة بتحديد هوية المتعاملين وأساليب التعامل وكيفيته، على عكس المعاملات التقليدية، إذ يأتي عاملي الثقة والأمان لدى المتعاملين في مقدمة الضمانات التي يتعين توافرها لتعزيز التعاملات الإلكترونية.

نتيجة لذلك استحدثت تشريعات الإثبات الإلكتروني كل من التصديق والحفظ الإلكترونيين كوسيلتين فنيتين أقرهما القانون لحماية أدلة الإثبات الإلكترونية (المحررات والتواقيع الإلكترونية)، إذ يقومان بتأمين موثوقية الدليل الكتابي الإلكتروني من خلال ضمان سلامته من أي تعديل أو تحريف.

حيث يقوم الحفظ الإلكتروني بضمان سلامة المحرر الموقع إلكترونيا من أي تعديل أو تحريف وبقائه بنفس الشكل الذي تم إنشاؤه، أو إرساله أو تسلمه به، مع ضمان إمكانية استرجاعه في أي وقت **(مطلب أول)**.

في حين يقوم التصديق الإلكتروني على التيقّن من إرادة كل طرف في المعاملة الإلكـــترونية، ومدى صحتها ونسبتها إلى من صدرت منه، وبعــدها عن الغــش والاحتيـــال، وكذلك التأكّد من طبيعة التعاقد وسلامة البيانات الإلكترونية المتصلة بالمحرر الإلكتروني، من أي تعديل أو تغيير فيه **(مطلب ثان)**.

ونظرا للأهمية العملية لكل من التصديق والحفظ الإلكترونيين سارعت تشريعات الإثبات الإلكتروني إلى تحديد نظامهما القانوني من خلال بيان دور كل منهما في تأمين أدلة الإثبات الإلكتروني، وعلى الرغم من أن آلية الحفظ الإلكتروني تعتبر عملية لاحقة لآلية عمل التصديق الإلكتروني إلا أننا ارتأينا التطرق إلى الدور الذي يلعبه الحفظ الإلكتروني في حماية أدلة

الإثبات الإلكتروني، لنبين فيما يلي دور التصديق الإلكتروني في هذه العملية وذلك للحفاظ على تسلسل الأفكار في هذه الدراسة.

المطلب الأول
الحفظ الإلكتروني

لكي يعتبر المحرر الإلكتروني دليلا كاملا في الإثبات وجب الاحتفاظ به بالشكل الأصلي الذي أنشأ به والمتفق عليه من قبل أطرافه، إذ تؤكد عملية الحفظ الإلكتروني على ضمان سلامة المعلومات الواردة في المحرر الإلكتروني من أي تغيير في شكلها الأصلي الذي أنشأت به، أو أرسلت أو استلمت عليه، مع ضمان إمكانية استرجاعه في أي وقت بذات الشكل الذي تم إنشاؤه أو إرساله أو تسلمه عليه، دون أي تحريف أو تبديل أو تغيير.

ونلاحظ أن هذا الشرط يقابل شرط ثبات الكتابة وعدم قابليتها للتعديل إلا بإتلاف المحـــرر، أو ترك أثر مادي عليه، ذلك أن حجية المحرر التقليدي في الإثبات تتوقف على ضمان سلامته المادية من أي تعديلات قد تؤثر على قوته في الإثبات؛ كالمحو، أو الكشط، أو التحشير، أو غير ذلك.

ومن ثم فإن تنظيم المسائل المرتبطة بتحديد مفهوم الحفظ الإلكتروني **(فرع أول)**، وشروط قيامه **(فرع ثان)**، وكذا المسؤول عنه **(فرع ثالث)** يُعد من الأمور الضرورية والمهمة التي وجب على تشريعات الإثبات الإلكتروني التطرق إليها، إلا أننا فوجئنا بقصور ونقص تنظيم لها سواء على المستوى الدولي أو الوطني، وهذا ما سيتم تفصيله فيما يلي.

الفرع الأول
تعريف الحفظ الإلكتروني

على الرغم من أهمية نظام الحفظ الإلكتروني في ضمان صحة أدلة الإثبات الإلكترونـــي، إلا أن أغلبية التشريعات الحديثة لم تهتم بإعطاء تعريف واضح له، وإنما اكتفت بالنص عليه وتحديد شروط قيامه، واقتصر تعريفه على ما جاء به بعض الفقه وكذا بعض القوانين.

اعتبر البعض أن حفظ المحرر والتوقيع الإلكترونيين يقصد به تخزين البيانات الإلكترونية الخاصة بهما ووضعها على دعامة ثابتة بحيث لا يمكن تغييرهما إلا من طرف المحتفظ بهـــا، كما لا يستطيع الغير الوصول لهذا التوقيع إلا بمعرفة صاحبه [1]، وينطوي هذا التعريف على شقين، يتمثل الشق الأول في وجوب تحميل بيانات التوقيع الإلكتروني على دعامة تخزين مناسبة وآمنة وذات طاقة تخزينية كافية[2]، أما الشق الثاني فيتمثل في الاحتفاظ بالدعامة الإلكترونية المحمل عليها بيانات التوقيع الإلكتروني بعيدا عن علم الغير، وأن لا تصل هذه البيانات للغير إلا بعلم وإرادة صاحب التوقيع.

أما بالنسبة لعلم المكتبات فقد شاع مصطلح آخر يدل على الحفظ الإلكتروني ألا وهو "الأرشفة الإلكترونية"[3]، وقد عرّفها النادي العربي للمعلومات بأنها: «**مسح الوثائق ومعالجتها وتخزينها في وسائط إلكترونية وربط هذه الوسائط بقاعدة بيانات الفهرس والكشاف بما يسمح بالنفاذ مباشرة من الفهرس أو الكشاف إلى صورة الوثيقة مباشرة**» [4].

---

(1)- **محمد سعيد أحمد إسماعيل**، أساليب الحماية القانونية لمعاملات التجارة الإلكترونية-دراسة مقارنة-، رسالة لنيل درجة دكتوراه، جامعة دمشق، 2005، ص 330.

(2)- GAUTRAIS Vincent, Le contrat électronique international, op.cit., p114.

حدد المشرع المصري من خلال المادة (3/ب) من الائحته التنفيذية لقانون التوقيع الإلكتروني، بأن الدعامة تكون مناسبة إذا كانت طاقتها قادرة على استيعاب الطول الإلكتروني لمفتاح التشفير، والذي حددته المادة السالفة الذكر بأن لا يقل عن (2048) (BIT).

(3)- يرى البعض ونحن نتفق معهم، بأنه على الرغم من ترابط مفهومي الحفظ الإلكتروني والأرشفة الإلكترونية إلا أنهما يختلفان من ناحية أن الأرشفة الإلكترونية تتعلق بكل المحررات، سواء التي ترتب آثارا قانونية أو لا، في حين أن الحفظ الإلكتروني يمس المحررات التي تنتج آثارا قانونية فقط. أنظر في ذلك:

Sébastien SOYEZ, Directives pour la gestion et l'archivage numérique des e – mails, Version 1.0, Bruxelles, 2008, disponible sur : https://francearchives.fr/file/a021ab377ae13a2d24d5467ef932c906d0c6c0cd/static_2823.pdf

(4)- **أحمد بن عبد الله الغرابي**، الأرشفة الإلكترونية في المملكة العربية السعودية " دراسة لواقع الوزارات والمؤسسات شبه الحكومية"، مطبوعات مكتبة الملك فهد الوطنية، السلسلة الأولى، الرياض، 2008، ص 31، مشار إليه لدى **باهة فاطمة**، مرجع سابق، ص 283.

بينما عرفه المعهد الفرنسي للتقييس **AFNOR** [1] على أنه: «**مجموعة من الإجراءات والأدوات والأساليب المستخدمة للحفظ المتوسط والطويل الأجل للمعلومات من أجل استغلالها**».

أما على المستوى التشريعي فقد نص قانون اليونسترال النموذجي بشأن التجارة الإلكترونية لعام (1996) من خلال المادة (1/10) منه المتعلقة بالاحتفاظ برسائل البيانات إذ نصت على: «**1- عندما يقتضي القانون بالاحتفاظ بمستندات أو سجلات أو معلومات بعينها، يتحقق الوفاء بهذا المقتضى إذا تم الاحتفاظ برسائل البيانات، شريطة مراعاة الشروط التالية:**

أ- تيسير الاطلاع على المعلومات الواردة فيها على نحو يتيح استخدامها في الرجوع إليها لاحقا؛ و

ب- الاحتفاظ برسالة البيانات بالشكل الذي أنشئت أو أرسلت او استلمت به أو بشكل يمكن إثبات أنه يمثل بدقة المعلومات التي أنشئت أو أرسلت أو استلمت؛ و

ج- الاحتفاظ بالمعلومات، إن وجدت، التي تمكن من استبانة منشأ رسالة البيانات وجهة وصولها وتاريخ ووقت إرسالها واستلامها...».

نلاحظ من خلال نص هذه المادة أن قانون اليونسترال النموذجي بشأن التجارة الإلكترونية لعام (1996) لم يقدم تعريفا للحفظ الإلكتروني، وإنما ركز على تنظيم آلية عمله من خلال تبيان شروط الاحتفاظ برسائل البيانات حتى يحتج بها في الاثبات.

أما عن التنظيم الأوروبي (910-2014) سالف الذكر، فلم يقدم هو الآخر تعريفا للحفظ الإلكتروني وإنما نص على إسناد هذه المهمة لمقدمي خدمة الثقة، حيث نص من خلال المادة

---

(1)- يقصد بمصطلح **AFNOR (Association Française De Normalisation)**، المعهد الفرنسي للتقييس، أنشأ سنة (1926)، معترف به من قبل السلطات العامة، يعمل على تنسيق عملية تطوير المعايير وتعزيز تطبيقها، كما يعتبر النواة المركزية لنظام التقييس الفرنسي https://www.iso.org

(16/03) منه على أن: «**خدمة الثقة: هي خدمة إلكترونية تقدم عادة بمقابل مالي وتتمثل فيما يلي:**

أ- انشاء والتحقق والتثبت من التوقيعات الإلكترونية ومن الأختام الإلكترونية ومن الطوابع الزمنية الإلكترونية ومن خدمات الارسال الموصى عليه بالإضافة إلى الشهادات المتعلقة بهذه الخدمات.

ب- إنشاء والتحقق والتثبت من الشهادات لأجل توثيق مواقع الانترنت.

ج- حفظ التوقيعات الإلكترونية والأختام الإلكترونية أو الشهادات المتعلقة بهذه الخدمات»[1].

ما تجدر الإشارة إليه في هذا المقام، أن المشرع الأوروبي قد استبدل مصطلح مقدمي خدمات التصديق الإلكتروني الذي كان يستعمله بموجب التوجيه الأوروبي (1999/93) الملغى بموجب التنظيم الأوروبي (2014/910) بمصطلح مزود خدمات الثقة؛ ذلك أن مهام هذه الفئة لا تقتصر على خدمة التصديق فقط، وإنما تتعدى ذلك إلى خدمات أخرى كالتحقّق والتثبت وكذا الحفظ الإلكتروني.

أما بالنسبة للتشريعات الوطنية التي اهتمت بعملية الحفظ الإلكتروني فنجد المشرع التونسي الذي نظّم عملية الحفظ الإلكتروني من خلال القانون (83-2000) المتعلق بالمبادلات والتجارة الإلكترونية، حيث نص في الفصل الرابع منه من الباب الثاني المعنون ب " **في الوثيقة الإلكترونية والإمضاء الإلكتروني**" على ما يلي: «**يعتمد قانونا حفظ الوثيقة الإلكترونية كما يعتمد حفظ الوثيقة الكتابية، ويلتزم المرسل بحفظ الوثيقة الإلكترونية في الشكل المرسلة به، ويلتزم المرسل إليه بحفظ هذه الوثيقة في الشكل الذي تسلمها به.**

ويتم حفظ الوثيقة الإلكترونية على حامل إلكتروني يمكّن من:

---

(1)- Article 03/16 du règlement n° 910-2014 : **«service de confiance», un service électronique normalement fourni contre rémunération qui consiste:**

a) en la création, en la vérification et en la validation de signatures électroniques, de cachets électroniques ou d'horodatages électroniques, de services d'envoi recommandé électronique et de certificats relatifs à ces services;

b) ou en la création, en la vérification et en la validation de certificats pour l'authentification de site internet;

c)ou en la conservation de signatures électroniques, de cachets électroniques ou des certificats relatifs à ces services».

-الاطلاع على محتواها طيلة مدة صلاحيتها،

- حفظها في شكلها النهائي بصفة تضمن سلامة محتواها،

- حفظ المعلومات الخاصة بمصدرها ووجهتها وكذلك تاريخ ومكان إرسالها أو استلامها».

من خلال هذه المادة يتبين أن المشرع التونسي قد استند على نص المادة (10) من قانون اليونسترال النموذجي لسنة (1996) بشأن التجارة الإلكترونية في تحديد شروط الحفظ الإلكتروني.

نجد المشرع المصري قد نص من خلال المادة (18/أ) من اللائحة التنفيذية لقانون التوقيع الإلكتروني على ضرورة توافر خدمة الحفظ الإلكتروني للاعتراف بحجية الكتابة والمحررات الإلكترونية في الإثبات، حيث نص على أنه: «**... تتحقق حجية الإثبات المقررة للكتابة الإلكترونية والمحررات الرسمية والعرفية لمنشئها، إذا توافرت الضوابط الفنية والتقنية الآتية: أ- إذا كان متاحا فنيا تحديد وقت وتاريخ إنشاء الكتابة الإلكترونية أو المحررات الإلكترونية الرسمية أو العرفية، وأن تتم هذه الإتاحة خلال نظام حفظ إلكتروني مستقل وغير خاضع لسيطرة منشئ هذه الكتابة أو تلك المحررات أو لسيطرة المعني بها».**

مقارنة بين التشريعين، نلاحظ أن المشرع التونسي قد توسّع أكثر من المشرع المصري في تنظيم شروط الحفظ الإلكتروني، إذ اقتصر هذا الأخير على ذكر شرطين فقط.

أما عن المشرع الفرنسي فقد اشترط من خلال المادة (1366) من القانون المدني الفرنسي، على أنه لكي تمنح الكتابة الإلكترونية نفس القوة الثبوتية للكتابة الورقية يجب أن تحدّد هوية مصدرها، وكذا أن تحفظ في ظروف تضمن سلامتها [1]، ليتطرق كذلك إلى هذا الشرط من خلال المرسوم رقم (71-941) المتعلق بالمحررات المنشئة من قبل الموثقين

(1)- Article 1366 du code civil français: «**L'écrit électronique a la même force probante que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité»** Modifié par Ordonnance n°2016-131 du 10 février 2016 - art. 4.

بخصوص حفظ المحررات المنشأة على دعامة إلكترونية، إذ نص من خلال المادة (28) منه على ضرورة حفظها في شروط من طبيعتها أن تحافظ على السلامة وسهولة القراءة.

كما نص على هذا الشرط كذلك من خلال المرسوم (972-2005) [1] بشأن المحرر الرسمي الإلكتروني وحفظه بواسطة المحضرين القضائيين، حيث أوضح من خلال المادة (5) منه على وجوب قيام المحضر القضائي بحفظ المحرر الرسمي الإلكتروني بواسطة نظام معالجة وحفظ ونقل المعلومات، وأن يكون النظام معتمدا من قبل منظمة المحضرين القضائيين، وأن يضمن –هذا النظام– خصوصية محتوى المحرر الرسمي الإلكتروني وسلامته من أي تحريف أو تزوير أو تلف.

فيما نص المشرع المغربي في الفقرة الثانية من الفصل (1-417) من قانون الالتزامات والعقود، والتي أضيفت بموجب القانون رقم (05-53) المتعلق بالتبادل الإلكتروني للمعطيات القانونية على أنه: «... **تقبل الوثيقة المحررة بشكل إلكتروني للإثبات، شأنها في ذلك شأن الوثيقة المحررة على الورق، شريطة أن يكون بالإمكان التعرف، بصفة قانونية، على الشخص الذي صدرت عنه وأن تكون معدة ومحفوظة وفق شروط من شأنها ضمان تماميتها**»، إلا أننا عند استقراء باقي المواد نجد أن المشرع المغربي لم يتطرق للشروط التي تضمن تمامية الوثيقة الإلكترونية المحفوظة.

أما بالنسبة للمشرع الجزائري فأول ما تعرض لشرط الحفظ الإلكتروني كان من خلال تعديل القانون المدني لسنة (2005) بموجب المادة (323 مكرر 1) حيث نص من خلالها على أنه: «**يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق، بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها**» [2].

---

(1)- Décret n° 2005-972 du 10 août 2005 modifiant le décret n° 56-222 du 29 février 1956 pris pour l'application de l'ordonnance du 2 novembre 1945 relative au statut des huissiers de justice, JORF n°186 du 11 août 2005 page 13095 texte
n° 33. https://www.legifrance.gouv.fr/

(2)– مصطلح السلامة هو ترجمة للمصطلح الأنجلوساكسوني "**integrity**"، ويقصد به من الناحية اللغوية حالة الشيء الذي يحفظ على حاله سليما دون أن يتعرض لأي إنقاص أو تعديل أو تدمير لخصائصه أو لحالته الأصلية.

لينص –وبعد حوالي عشر سنوات– من خلال القانون (15–04) المتعلق بالتوقيع والتصديق الإلكترونيين بموجب المادة (4)[1]منه على وجوب حفظ الوثيق الموقعة إلكترونيا، وفقا للتشريع والتنظيم المحدد لذلك.

وإفراغا لنص هذه المادة تم إصدار المرسوم التنفيذي رقم (16–142) بتاريخ (05 ماي 2016) المحدد لكيفيات حفظ الوثيقة الموقعة إلكترونيا[2]، وهو المرسوم الذي تضمن (10) مواد بَيَّن من خلالها المشرع الجزائري كيفية حفظ الوثيقة الإلكترونية، المسؤول عن عملية الحفظ، وكذا مدة الحفظ.

تطرق المشرع الجزائري من خلال المرسوم أعلاه المحدد لكيفيات حفظ الوثيقة الموقعة إلكترونيا إلى المقصود بآلية الحفظ من خلال المادة (2) منه، ونص على أنها: «**مجموعة التدابير التقنية التي تسمح باستلام وحفظ واسترجاع الوثيقة الموقعة إلكترونـــيا**»، ليعرف كذلك من خلال المادة نفسها دعامة الحفظ بأنها: «**أي وسيلة مادية، أيا كان شكلها أو خصائصها المادية، تسمح باستلام وحفظ واسترجاع الوثيقة الموقعة إلكترونيا**».

يتضح لنا من خلال ما تطرقنا إليه أن المشرع الجزائري هو الوحيد الذي أفرد لآلية الحفظ الإلكتروني مرسوما تنظيميا خاصا، في حين أن باقي التشريعات التي سبق لنا ذكرها قد نظمت هذه العملية إما من خلال قوانينها المتعلقة بالإثبات الإلكتروني، أو من خلال نصوص متفرقة في قوانين مختلفة.

–dictionnaire Larousse, le terme intégrité, disponible sur http://www.larousse.fr/dictionnaires/francais/int%C3%A9grit%C3%A9/43543

(1)– تنص المادة 4 من القانون 15–04 المتعلق بالتوقيع والتصديق الإلكترونيين على: «**تحفظ الوثيقة الموقعة إلكترونيا في شكلها الأصلي. ويتم تحديد الكيفيات المتعلقة بحفظ الوثيقة الموقعة إلكترونيا عن طريق التنظيم**».

(2)– مرسوم تنفيذي رقم 16–142 مؤرخ في 27 رجب عام 1437 الموافق 5 مايو سنة 2016، يحدد كيفيات حفظ الوثيقة الموقعة إلكترونيا، ج. ر.ع 28 صادر بتاريخ 8 مايو سنة 2016.

الفرع الثاني
شروط الحفظ الإلكتروني

يلاحظ من خلال القراءة الأولية للنصوص القانونية التي أسلفنا ذكرها في بيان مفهوم الحفظ الإلكتروني، أنه يمكن حصر شروط حفظ الوثيقة الإلكترونية في ثلاثة؛ تتعلق الأولى ببيانات الوثيقة الإلكترونية **(أولا)**، في حين تختص الثانية بدعامة الحفظ **(ثانيا)**، أما عن الثالثة فهي تتعلق بمدة الحفظ **(ثالثا)**، وسنتطرق بالتفصيل لكل واحدة من هذه الشروط فيما يلي.

أولا: شروط تتعلق ببيانات الوثيقة الإلكترونية

تنص المادة (10) من قانون اليونسترال النموذجي بشأن التجارة الإلكترونية لعام (1996) على أنه: **«1- عندما يقتضي القانون بالاحتفاظ بمستندات أو سجلات أو معلومات بعينها، يتحقق الوفاء بهذا المقتضى إذا تم الاحتفاظ برسائل البيانات، شريطة مراعاة الشروط التالية:**

أ- تيسير الاطلاع على المعلومات الواردة فيها على نحو يتيح استخدامها في الرجوع إليها لاحقا؛ و

ب- الاحتفاظ برسالة البيانات بالشكل الذي أنشئت أو أرسلت أو استلمت به أو بشكل يمكن إثبات أنه يمثل بدقة المعلومات التي أنشئت أو أرسلت أو استلمت؛ و

ج- الاحتفاظ بالمعلومات، إن وجدت، التي تمكن من استبانة منشأ رسالة البيانات وجهة وصولها وتاريخ ووقت إرسالها واستلامها...».

كما تنص المادة (8) من قانون المعاملات الإلكترونية الأردني (15 لسنة 2015) على أنه: **«إذا استوجب القانون الاحتفاظ بمستند لأي سبب فيعتبر الاحتفاظ به على شكل سجل إلكتروني منتجا لآثاره على أن تتوافر فيه الشروط المنصوص عليها في المادة 7 من هذا القانون».** أما عن الشروط التي ذكرت فينص المادة (8) فبالعودة للمادة (7) من القانون نفسه نجدها تنص على أنه: **«إذا اشترط أي تشريع تقديم النسخة الأصلية من أي قيد أو عقد أو مستند أو وثيقة فيعتبر السجل الإلكتروني مستوفيا لهذا الشرط بتوافر ما يلي:**

1 – حفظه بالشكل الذي تم به إنشاؤه أو إرساله أو تسلمه وبشكل يضمن عدم إجراء أي تغيير أو تعديل على محتواه.

2 – حفظه على نحو يتيح الوصول إلى المعلومات الواردة فيه واستخدامها والرجوع إليها في أي وقت.

3 – التمكن من التعرف على المنشئ والمرسل إليه وتاريخ ووقت إنشائه أو إرساله أو تسلمه...».

استنادا إلى ما سبق ذكره من نصوص قانونية، نستخلص أن الشروط القانونية الواجب توافرها في آلية الحفظ الإلكتروني حتى يُعتد بها في الإثبات، تتمثل في وجوب الاحتفاظ برسالة البيانات في شكلها الأصلي الذي أنشئت أو أرسلت أو استلمت به، مع ضمان عدم إجراء أي تعديل أو تغيير عليها، مع إمكانية الرجوع إلى المعلومات في أي وقت، إضافة إلى إمكانية التعرف على منشئ ومستلم الرسالة وتاريخ ووقت إرسالها واستلامها.

وبالرجوع للقانون الجزائري نجد أن المشرع الجزائري نص من خلال المادة (3) من المرسوم التنفيذي (16–142) سالف الذكر على أنه: «**يجب أن يضمن حفظ الوثيقة الموقعة إلكترونيا استرجاع هذه الوثيقة في شكلها الأصلي لاحقا، والتحقق من توقيعها الإلكتروني**».

لتنص فيما بعد المادة (4) من المرسوم نفسه على البيانات الواجب حفظها في الوثيقة الموقع إلكترونيا، إذ تنص هذه المادة على أنه: «**يجب أن يتضمن حفظ الوثيقة الموقعة إلكترونيا على الخصوص ما يأتي:**

- **الوثيقة الإلكترونية وتوقيعها الإلكتروني، أيا كان مرفقا أو متصلا بشكل منطقي،**
- **شهادة التصديق الإلكتروني للموقع،**
- **قائمة الشهادات الإلكترونية الوسيطة إلى غاية الوصول إلى السلطة الوطنية للتصديق الإلكتروني، عندما يتعلق الأمر بشهادة إلكترونية موصوفة، قوائم الشهادات الملغاة أو نتائج التحقق من حالة الشهادات الإلكترونية الوسيطة إلى غاية الوصول للسلطة الوطنية للتصديق الإلكتروني،**

- **تاريخ توقيع الوثيقة، عند الاقتضاء».**

عند استقراء هذه المادة لا نجدها تنص فقط على الشروط القانونية الواجب توافرها في آلية الحفظ الإلكتروني للاعتداد بها في الإثبات؛ كالوثيقة الإلكترونية وتوقيعها الإلكتروني، إضافة إلى تاريخ توقيع الوثيقة مثلما نصت القوانين سالفة الذكر؛ وإنما تنص أيضا على الوثائق الإلكترونية الواجب حفظها والتي تتمثل في كل من الوثيقة الإلكترونية الموقّعة إلكترونيا، شهادة التصديق الإلكتروني للموقّع، قائمة الشهادات الإلكترونية الوسيطة....

لذا حبذا لو أعاد المشرع الجزائري النظر في صياغة هذه المادة القانونية لتتماشى مع الشروط الواجب توفرها في آلية الحفظ الإلكتروني ليُعتد به في الإثبات، وأن يستأنس في ذلك إلى ما جاء به قانون اليونسترال النموذجي بشأن التجارة الإلكترونية لسنة (1996).

ثانيا: الشروط المتعلقة بدعامة الحفظ

عرّف المشرع الجزائري "دعامة الحفظ" من خلال المادة (2) من المرسوم التنفيذي (16-142) سالف الذكر على أنها: **«أي وسيلة مادية، أيّا كان شكلها أو خصائصها الماديـــة، تسمح باستلام وحفظ واسترجاع الوثيقة الموقعة إلكترونيا».**

في حين عرّفها المشرع المصري من خلال المادة (14/1) من اللائحة التنفيذية لقانون التوقيع الإلكتروني لسنة (2004) على أنها: **«وسيط مادي لحفظ وتداول الكتابة الإلكتـرونية، ومنها الأقراص المدمجة أو الأقراص الضوئية أو الأقراص الممغنطة أو الذاكرة الإلكترونية أو أي وسيط آخر مماثل».**

من خلال هذين التعريفين نصل إلى أن وجوب توافر خاصية الثقة والثبات في الدعامة الإلكترونية طول فترة الحفظ، لضمان عدم المساس بها أو إجراء أي تعديلات عليها، كما نلاحظ أيضا أن المشرع الجزائري لم يقدم أي أمثلة عن شكل الدعامة وإنما ترك المجال مفتوحاً أمام أي وسيلة مادية؛ أيا كان شكلها؛ بإمكانها تحقيق عملية الحفظ الإلكتروني. في حين أن

المشرع المصري تطرق للبعض منها؛ كالأقراص المدمجة أو الضوئية أو الممغنطة، أو الذاكرة الإلكترونية، ليفتح هو الآخر المجال لأي وسيلة تمكّن من تحقيق عملية الحفظ الإلكتروني.

كما اشترط المشرع الجزائري من خلال المادة (6)[1] من المرسوم التنفيذي (16-142) سالف الذكر، على أن تتم عملية الحفظ الإلكتروني من خلال دعامة تسمح بالنفاذ إلى محتواها واسترجاعه في أي وقت، باستخدام الوسائل التقنية الملائمة، واشترط كذلك من خلال الفقرة الثانية من المادة نفسها على الاستغلال الحسن لهذه الدعامات من قبل الأشخاص المسؤولين عن عملية الحفظ.

إضافة إلى ذلك نص المشرع الجزائري من خلال المادتين (7) و(8) [2] من المرسوم ذاته على أنه في حال نقل الوثيقة الموقّعة إلكترونيا من دعامة حفظ لأخرى، أن تنقل جميع العناصر الواردة في المادة (4) [3]، وأن يتحقق من التوقيع الإلكتروني بعد كل عملية نقل، كما اشترط وجوب استرجاع الوثيقة في شكلها الأصلي دون أي تعديل أو تغيير.

---

(1)- تنص المادة (6) من المرسوم التنفيذي (16-142) السالف الذكر على أنه: **«يتم حفظ الوثيقة الموقعة إلكترونيا على دعامة حفظ يسمح في أي وقت بالنفاذ إلى محتواها واسترجاعها بواسطة الوسائل التقنية الملائمة.**

يجب على الأشخاص المذكورين في المادة 5 أعلاه، استعمال دعامات الحفظ وفق الشروط التي تضمن سلامتها وسيرها الحسن».

(2)- تنص المادة (7) من المرسوم التنفيذي (16-142) على أنه: **«يجب أن يشمل نقل الوثيقة الموقعة إلكترونيا من دعامة حفظ إلى دعامة أخرى، جميع العناصر الواردة في المادة 04 أعلاه.**

يجب التحقّق من التوقيع الإلكتروني بعد نقل الوثيقة الموقعة إلكترونيا إلى دعامة حفظ جديدة»

تنص المادة (8) من المرسوم (16-142) على أنه: **«يجب أن تضمن كل عملية تجري على الوثيقة الموقعة إلكترونيا والمحفوظة، لدواعي الفعالية و/ أو الأمن، استرجاعها في شكلها الأصلي».**

(3)- تنص المادة (4) من المرسوم التنفيذي (16-142) على أنه: **«يجب أن يتضمن حفظ الوثيقة الموقعة إلكترونيا على الخصوص ما يأتي:**

- **الوثيقة الإلكترونية وتوقيعها الإلكتروني، أيا كان مرفقا أو متصلا بشكل منطقي،**
- **شهادة التصديق الإلكتروني للموقع،**
- **قائمة الشهادات الإلكترونية الوسيطة إلى غاية الوصول إلى السلطة الوطنية للتصديق الإلكتروني، عندما يتعلق الأمر بشهادة إلكترونية موصوفة، قوائم الشهادات الملغاة أو نتائج التحقق من حالة الشهادات الإلكترونية الوسيطة إلى غاية الوصول للسلطة الوطنية للتصديق الإلكتروني،**

ثالثا: مدة الحفظ الإلكتروني

تنص المادة (9) من المرسوم (16-142) سالف الذكر، على أنه: «**دون المساس بالتشريع والتنظيم المعمول بهما، يتم حفظ الوثيقة الموقعة إلكترونيا خلال مدة منفعتها**»، نستخلص من هذا النص أن المشرع الجزائري قد اشترط حفظ المحررات الموقعة إلكترونيا لمدة معيّنة تتعلق أساسا بصلاحية المحرر. وعليه ترتبط مدة حفظ المحررات الإلكترونية بمدة تقادمها على أقل تقدير إذ لا مانع من استمرار مدة الحفظ لفترة أطول، لا سيما في وجود البطاقات الذكية ذات السعة العالية التي لا تتأثر بمضي الزمن على تحميلها للبيانات.

ينشأ المحرر الإلكتروني بناء عن معاملة مدنية أو تجارية أو مختلطة، ورجوعا للقواعد العامة نجد أن مدد التقادم المنصوص عليها في القانون المدني تختلف باختلاف الحق المتنازع عليه وذلك وفقا للمادة (308) وما يليها من القانون المدني الجزائري، إذ يمكن أن تكون مدة التقادم سنوية أو ثلاثية أو خماسية أو طويلة تقدر ب (15) سنة.

أما عن المواد التجارية فيلتزم الطرفان بحفظ المحرر الإلكتروني وفقا للمدة التي حددها القانون بغض النظر عن مدة تقادم الحق أو الالتزام الوارد في المحرر، وقد نصت المادة (12) من القانون التجاري الجزائري سالف الذكر على أنه: «**يجب أن تحفظ الدفاتر والمستندات المشار إليها في المادة (9) و(10) لمدة عشر سنوات، كما يجب أن ترتب وتحفظ المراسلات الواردة ونسخ الرسالات الموجهة طيلة نفس المدة**».

أما عن القاعدة العامة التي تحكم المعاملة التجارية المختلطة؛ والتي تكون مدنية لطرف وتجارية للطرف الآخر، فيسري على كل منهما القواعد التي تخصه، وعليه يلتزم كل منهما بالحفظ الإلكتروني وفقا للقواعد الخاصة به [1].

- **تاريخ توقيع الوثيقة، عند الاقتضاء**».

(1)- باهة فاطمة، مرجع سابق، ص 301.

وعلى خلاف ما تم توضيحه سابقا، فإن حفظ التوقيعات الإلكترونية لا ترتبط بمدة معينة، فصاحب التوقيع الإلكتروني ملزم بحفظ توقيعه الإلكتروني بشكل دائم منعا لاستخدامه غير المشروع من قبل الغير، وكذا لأن الأصل في التوقيع أنه لا ينتهي بمدة تقادم.

الفرع الثالث

المسؤول عن عملية الحفظ الإلكتروني

أسندت بعض تشريعات الإثبات الإلكتروني مهمة حفظ الوثيقة الإلكترونية إلى صاحبها، لما له من مصلحة في حمايتها من أي عبث أو ضياع، إلا أن ما تتطلبه عملية الحفظ من مهارة تقنية قد لا تتوفر في صاحب الوثيقة الإلكترونية، دفع بعض المشرعين إلى إسناد هذه المهمة إلى طرف ثالث يقوم بعملية الحفظ الإلكتروني بدلا من صاحب الوثيقة، في حين نصت بعض التشريعات على إسناد هذه المهمة أساسا إلى صاحب الوثيقة، ويمكنه أن يستعين في حفظها بطرف ثالث موثوق.

نص قانون اليونسترال النموذجي بشأن التجارة الإلكترونية لسنة (1996) من خلال المادة (3/10) على أنه: «... **يجوز للشخص أن يستوفي المقتضى المشار إليه في الفقرة (1) بالاستعانة بخدمات أي شخص آخر، شريطة مراعاة الشروط المنصوص عليها في الفقرات الفرعية (أ) و(ب) و(ج) من الفقرة (1)**».

نستشف من خلال هذا النص، أن قانون اليونسترال النموذجي بشأن التجارة الإلكترونية لسنة (1996) لم يحدد المقصود " **بالشخص الآخر**" الذي مكّن من الاستعانة به في حفظ المستندات أو السجلات أو المعلومات، وهذا الأمر نرى أنه قد يُعاب على مشرع قانون اليونسترال باعتباره قانون نموذجي في مجال تنظيم المعاملات الإلكترونية.

خلافا لقانون اليونسترال النموذجي بشأن التجارة الإلكترونية لعام (1996)، نجد أن التنظيم الأوروبي رقم (2014/910) المتعلق بتحديد الهوية الإلكترونية وخدمات الثقة في المعاملات الإلكترونية داخل السوق الداخلي سالف الذكر، قد حدد صراحة الجهة المسؤولة عن عملية الحفظ الإلكتروني وهي ذات الجهة المسؤولة عن عملية التصديق الإلكتروني والتي أطلق

عليها مصطلح "**مقدم خدمات الثقة**"، حيث عرّفه من خلال المادة (19/3) من التنظيم نفسه بأنه: «... **شخص طبيعي أو معنوي يقدم خدمة واحدة أو أكثر من خدمات الثقة، كما يمكن أن يكون موصوف أو غير موصوف**»[1]، وقد نص هذا التنظيم صراحة من خلال المادة (16/3)[2] منه، على أن من بين صور خدمة الثقة حفظ التوقيعات والأختام والشهادات الإلكترونية وذلك نظير مقابل مالي.

ويبدو أن المشرع الفرنسي قد انتهج نفس منهج التنظيم الأوروبي، ذلك من خلال توسيع مهام مقدم خدمة الثقة لتشمل خدمات التصديق والحفظ والتحقق من التوقيعات الإلكترونية، وذلك حين عرفه بأنه كل شخص يوفّر الخدمات التي تهدف إلى تنفيذ الوظائف التي تساهم في تأمين الأنظمة المعلوماتية والمعلومات المتبادلة بالطريق الإلكتروني [3].

بينما نجد أن المشرع التونسي قد أسند مهمة الحفظ الإلكتروني لكل من المرسل والمرسل إليه، وذلك من خلال الفصل (4) من القانون (83 لسنة 2000) سالف الذكر، إذ نص على أنه: «**يعتمد قانونا حفظ الوثيقة الإلكترونية كما يعتمد حفظ الوثيقة الكتابية.**

ويلتزم المرسل بحفظ الوثيقة الإلكترونية في الشكل المرسلة به، ويلتزم المرسل إليه بحفظ هذه الوثيقة في الشكل الذي تسلمها به...». نجد في مقابل ذلك؛ أن المشرع المصري ومن خلال لائحته التنفيذية لقانون التوقيع الإلكتروني؛ قد أسند هذه المهمة لنظام مستقل غير خاضع لسيطرة منشئ الكتابة أو المعني بها، إذ نص من خلال المادة (8/أ) من اللائحة

---

(1)- Article 03/19 du règlement n° 910-2014: «**…prestataire de services de confiance» , une personne physique ou morale qui fournit un ou plusieurs services de confiance, en tant que prestataire de services de confiance qualifié ou non qualifié;…** »

(2)- Article 03/16 du règlement n° 910-2014: «**…service de confiance», un service électronique normalement fourni contre rémunération qui consiste:**
a) en la création, en la vérification et en la validation de signatures électroniques, de cachets électroniques ou d'horodatages électroniques, de services d'envoi recommandé électronique et de certificats relatifs à ces services;
b) ou en la création, en la vérification et en la validation de certificats pour l'authentification de site internet;
c)ou en la conservation de signatures électroniques, de cachets électroniques ou des certificats relatifs à ces services…».

(3)- Eric A. CAPRIOLI, Les Tiers de Confiance, Preuve informatique : quelles nouveautés techniques pour quelles évolutions juridiques ? Bibliothèque de l'Ordre, Paris 8 décembre 2011 , p 09, disponible sur : http://www.adij.fr/wp-content/uploads/2012/01/ADIJ_Pre%CC%81sentation-Tiers-deconfiance-V2.pdf

التنفيذية لقانون التوقيع الإلكتروني على أنه: «... **أ- أن يكون متاحا فنيا تحديد وقت وتاريخ إنشاء الكتابة الإلكترونية أو المحررات الإلكترونية الرسمية أو العرفية، وأن تتم هذه الإتاحة من خلال نظام حفظ إلكتروني مستقل وغير خاضع لسيطرة منشئ هذه الكتابة أو تلك المحـــررات، أو لسيطرة المعني بها...**»، إلا أن ما يعاب عليه هو الآخر عدم تحديد المكلف بهمة الحفظ الإلكتروني.

أما عن المشرع الجزائري فقد نص صراحة على أن المسؤول عن عملية الحفظ الإلكتروني هو صاحب المحرر في حد ذاته أو مستلم المحرر. ولأن عملية الحفظ الإلكتروني تتطلب مهارة وكفاءة عالية قد لا تتوفر في صاحب المحرر أو التوقيع الإلكترونيين، سمح المشرع باللجوء إلى طرف ثالث للقيام بعملية الحفظ، دون تحديد تشريعي واضح لهذا الطرف وفقا لما نصت عليه المادة (5)[1] المرسوم (16-142) سالف الذكر، إلا أن نص المشرع الجزائري على ضرورة حفظ الوثيقة الإلكترونية من خلال المادة (4) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين، يدفعنا إلى القول أن المقصود بالطرف الثالث في عملية الحفظ الإلكتروني هو نفسه المسؤول عن عملية التصديق الإلكتروني، وهذا ما اعتمدته أغلب التشريعات التي أوضحناها سابقا.

المطلب الثاني
التصديق الإلكتروني

تتميز المحررات التقليدية عن الإلكترونية بسمتين أساسيتين؛ تتمثل الأولى في وجود محرر مكتوب على وسيط مادي ليس من السهل إنكاره أو تغيير مضمونه، في حين ترتبط السمة الثانية بوجود توقيع يذيّل به المحرر يفيد صحته ونسبته لمن وقع عليه. وعلى الرغم من توافر هاتين السمتين في المحررات الإلكترونية، إلا أن الطبيعة اللامادية التي يتميزان بها تثير الكثير من الشكوك حول درجة الثقة والأمان المتوفرين في المحرر الإلكتروني، خصوصا في ظل تنامي القرصنة الإلكترونية، وإساءة استخدام أسماء الغير في تعاملات غير مشروعة عبر

(1)- تنص المادة (5) من المرسوم التنفيذي 16-142: «**يجب على كل شخص طبيعي أو معنوي موقع و/أو مستلم لوثيقة موقعة إلكترونيا، أن يضمن حفظها بنفسه أو عبر طرف ثالث**».

مختلف الوسائط الإلكترونية، هذا ما ينعكس بالنتيجة على القيمة القانونية للمحررات والتواقيع الإلكترونية في مجال الإثبات.

لذا بات من الضروري، التأكّد من صدور المعاملة الإلكترونية ممن تنسب إليه دون تعديل أو تحريف، وحلا لهذه المشاكل القانونية أوجدت قوانين الإثبات الإلكتروني الدولية والإقليمية والوطنية تقنية التصديق الإلكتروني، وهو عبارة عن "**وسيلة فنية آمنة للتحقق من صحة التوقيع أو المحرر الإلكتروني، حيث يتم نسبته إلى شخص أو كيـــان معيّن عبر جهـــة موثوق بهـــا، أو طرف محايد يطلق عليه اسم مقدم خدمات التصديق أو التوثيق الإلكتروني**"[1]. وهناك من اعتبره بأنه: "**إجراء عن طريق شخص ثالث أو جهة معتمدة عن طريق بعض الإجراءات الفنية، يهدف إلى تثبيت مضمون المحرر ودقة ما يحمله من توقيعات وصحة نسبته إلى من صدر عنه، ويضمن سلامة وتأمين التعامل عبر الإنترنت سواء من حيث أطرافه أو محله أو تأمينه**"[2].

وعليه، تتم عملية التصديق الإلكتروني عن طريق جهات محايدة يطلق عليها مقدم خدمات التصديق **(فرع أول)**، يمنح لها ترخيص أو تفويض من قبل هيئات عليا **(فرع ثـــان)**، بعد أن تستوف بعض الشروط والمتطلبات القانونية لتتمكنّ من ممارسة مهامها ووظائفها **(فرع ثالث)**.

الفرع الأول
الجهات المكلفة بتقديم خدمة التصديق الإلكتروني

اختلفت التسميات التي أطلقت على الجهات المكلفّة بتقديم خدمة التصديق الإلكتروني، إذ أطلق عليها البعض اسم مزود خدمات التصديق الإلكتروني، فيما أطلق عليها البعض الآخر اسم جهة التوثيق أو سلطات التصديق الإلكتروني، إلا أن المهم في الموضوع أنها تؤدي

(1)- أسامة بن غانم العبيدي، التصديق الإلكتروني وتطبيقاته في النظام السعودي، بحث محكم منشور في المجلة القضائية بالسعودية، العدد 04، رجب 1433، ص179.

(2)- زيد حمزة مقدم، وسائل وضمانات التوثيق الإلكتروني، مجلة جامعة بحري للآداب والعلوم الإنسانية، السودان، السنة 03، العدد 06، ديسمبر 2014، ص 171.

المعنى ذاته؛ وهو تدخل طرف ثالث معين من قبل سلطات الدولة أو من قبل الأفراد أو من جهات خاصة أخرى، مهمته بعث الثقة والأمان في المعاملات الإلكترونية التي تتم بين المتعاقدين. وعليه؛ يمكن القول أنه لا يوجد تعريف فقهي متفق عليه لجهات التصديق الإلكتروني، كما أنه لا توجد تسمية موحّدة لهذه الجهات في تشريعات الدول المختلفة.

تعددت التعاريف الفقهية لمؤدي خدمات التصديق الإلكتروني، فمنهم من عرّفه بأنه عبارة عن: **«هيئة أو مؤسسة عامة أو خاصة تستخرج شهادات إلكترونية تعدّ بمثابة سجّل إلكتروني يؤمن التوقيع الإلكتروني ويحدد هوية الموقع ومعرفة المفتا العـــام، كما تعتبر هذه الشهادة بمثابة بطاقة هوية إلكترونية تستخرج من شخص مستقل ومحايد ومرخص له بمزاولة النشاط»** [1].

ويعرّف جانب آخر من الفقه [2]، مؤدي خدمات التصديق بأنه: **«أي شخص أو جهة معتمدة أو معترف بها تقوم بإصدار شهادات تصديق إلكترونية أو أية خدمات أو مهمات متعلقة بها وبالتواقيع».**

في حين يعرّفها جانب ثالـث من الفقه [3]، بأنها: **«شخص طبيعي أو معنوي يستخرج الشهادات الإلكترونية ويقدم الخدمات الأخرى المرتبطة بالتوقيعات الإلكترونية، ويضمن تحديد هوية الأطراف المتعاقدة والاحتفاظ بهذه البيانات مدة معينة، ويلتزم باحترام القواعد المنظمة لعمله والتي يتم تحديدها بمعرفة السلطة المختصة».**

نلاحظ من هذه التعاريف؛ إجماعها؛ على المهمة الرئيسية التي تقوم بهـا هـذه الجهـات وهي إضفاء الثقة في التعاملات الإلكترونية المبرمة عبر الإنترنت والاحتفاظ بأصول

---

(1)- هلا الحسن، تصديق التوقيع الإلكتروني لجهة التوثيق الإلكتروني، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 30، العدد 01، سوريا، 2014 ، ص 40؛ **أنظر أيضا:**

BRUN-B, « Nature et impacts juridiques de la certification dans le commerce électronique sur internet », mars 2006, p 06.
http://www.lex-electronica.org

(2)-CAPRIOLO Eric, Règlement des litiges internationaux et droit applicable dans le commerce électronique, Paris 2002,p 56.

(3)- قنديل سعيد السيد، مرجع سابق، ص 75؛ **نجوى ابو هيبة**، مرجع سابق، ص 90.

التوقيعات الإلكترونية، وذلك بمسك أرشيف بها وتسليم المعنيين شهادات مصادقة إلكترونية، بالإضافة إلى بعض المهام الأخرى التي نتبينها عند تناولنا لدورها تفصيلا.

تناولت كذلك أغلب التشريعات التعريف بالجهات المكلفة بتقديم خدمة التصديق الإلكتروني، وفي مقدمتها قانون اليونسترال النموذجي بشأن التوقيعات الإلكترونية لعام (2001)، إذ عرّف من خلال المادة (2/هـ) منه مقدم خدمات التصديق الإلكتروني على أنه: **«شخص يصدر شهادات، ويجوز أن يقدم خدمات أخرى ذات صلة بالتوقيعات الإلكترونية».**

في حين أطلق عليه التنظيم الأوروبي رقم (2014/910) من خلال المادة (19/3)[1] مصطلح "مقدم خدمات الثقة" وعرّفه من خلال هذه المادة بأنه: **«مقدم خدمات الثقة: هو شخص طبيعي أو معنوي يقدم خدمة أو أكثر من خدمات الثقة، ويمكن أن يكون موصوف أو غير موصوف».** وعرف التنظيم الأوروبي من خلال الفقرة الموالية أي المادة (20/3)[2] مقدم خدمات الثقة الموصوف على أنه: **«...مقدم خدمات الثقة الموصوف: هو مقدم خدمات الثقة الذي يقدم خدمة أو أكثر من خدمات الثقة الموصوفة وحاصل على وضعية موصوف من قبل هيئة الرقابة»**، وقد أشار التنظيم الأوروبي من خلال المادة (16/3)[3] منه إلى مفهوم خدمة الثقة بأنها عبارة عن: **«خدمة إلكترونية تقدم عادة بمقابل مالي وتتمثل بما يلي:**

أ- إنشاء والتحقق والتثبت من التوقيعات الإلكترونية ومن الأختام الإلكترونية ومن الطوابع الزمنية الإلكترونية ومن خدمات الإرسال الموصى عليه الإلكتروني بالإضافة إلى الشهادات المتعلقة بهذه الخدمات؛

ب – إنشاء والتحقق والتثبت من الشهادات لأجل توثيق مواقع الإنترنت؛

ج- حفظ التوقيعات الإلكترونية والأختام الإلكترونية أو الشهادات المتعلقة بهذه الخدمات».

---

(1)- Article 03/19 du règlement n° 910-2014: «**…prestataire de services de confiance» , une personne physique ou morale qui fournit un ou plusieurs services de confiance, en tant que prestataire de services de confiance qualifié ou non qualifié;… ».**

(2)- Article 03/20 du règlement n° 910-2014: «**…prestataire de services de confiance qualifié», un prestataire de services de confiance qui fournit un ou plusieurs services de confiance qualifiés et a obtenu de l'organe de contrôle le statut qualifié;… »**

(3)- Article 03/16 du règlement n° 910-2014, op.cit.

بالرجوع للتشريعات الوطنية المقارنة نجد، أن المشرع التونسي قد أطلق عليه مصطلح "**مزود خدمات المصادقة الإلكترونية**" وعرّفه من خلال (الفصل 2) من القانون (83 لسنة 2000) المتعلق بالمبادلات والتجارة الإلكترونية بأنه: «**كل شخص طبيعي أو معنوي يحدث ويسلم ويتصرف في شهادات المصادقة ويسدي خدمات أخرى ذات علاقة بالإمضاء الإلكتروني**»، في حين أطلق عليه المشرع المغربي مصطلح " **مقدمو خدمات المصادقة الإلكترونية**" ونص عليهم بموجب المادة (20) من القانون (05-53) المتعلق بالتبادل الإلكتروني للمعطيات القانونية: «**مقدمو خدمات المصادقة الإلكترونية المعتمدون دون غيرهم، الذين يمكنهم إصدار شهادات إلكترونية مؤمنة، وتسليمها وتدبير الخدمات المتعلقة بها وفق الشروط المحددة في هذا القانون والنصوص المتخذة لتطبيقه**».

نلاحظ من خلال هذه النصوص القانونية، أنها عرفت "مقدم خدمات التصديق الإلكتروني" بالنظر للمهام التي يقوم بها، كما مكنّت الأشخاص الطبيعة والمعنوية على حد سواء من تقديم خدمات التصديق الإلكتروني، إضافة إلى ذلك لم تحصر مهمتهم في إصدار شهادات التصديق الإلكتروني، وإنما أجازت تقديم خدمات أخرى ذات صلة بالتوقيع الإلكتروني.

أما عن المشرع الأردني فقد استعمل مصطلح "**جهة التوثيق الإلكتروني**" وعرّفها من خلال المادة (14/2) من قانون المعاملات الإلكترونية الأردني رقم (15 لسنة 2015) على أنها: «**الجهة المرخصة أو المعتمدة من هيئة تنظيم قطاع الاتصالات أو المخولة قانونا بإصدار شهادات التوثيق وتقديم أي خدمات متعلقة بهذه الشهادات وفقا لأحكام هذا القانون والأنظمة والتعليمات الصادرة بموجبه**». في حين نجد أن المشرع المصري قد سماها ب: "**جهات التصديق الإلكتروني**" وعرّفها من خلال المادة (6/1) من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري رقم (15 لسنة 2015) بأنها: «...**الجهات المرخص لها بإصدار شهادة التصديق الإلكتروني وتقديم خدمات تتعلق بالتوقيع الإلكتروني**».

باستقراء هذين النصين، نجد أن كل من المشرع الأردني والمصري قد أوكل مهمة التصديق الإلكتروني إلى أشخاص معنوية وليست طبيعية، ولربما يعود ذلك في نظرهم إلى أن

تقديم خدمات التصديق الإلكتروني يحتاج إلى إمكانيات مادية وتقنية كبيرة، كما يحتاج إلى أجهزة معقدة وخبرات فنية كبيرة، قد لا تتوافر في الأشخاص الطبيعية.

أما فيما يتعلق بالمشرع الجزائري؛ ففقد نص على مصطلحين مختلفين في نصين قانونيين مختلفين لأجل التعريف بالجهة المخولة بتقديم خدمات التصديـــق الإلكترونـــي، فقد أطلق في النص القانوني الأول، على جهة التصديق مصطلح " **مؤدي خدمات التصديق الإلكتروني**"، بموجب نص المادة (3) من المرسوم التنفيذي (07-162) [1]: «**مؤدي خدمات التصديق خدمات التصديق الإلكتروني: كل شخص في مفهوم المادة 8-8 من القانون 2000-03 المؤرخ في05 أوت 2000 والمذكور أعلاه، يسلـــم شهـــادات إلكترونـــية أو يقدم خدمات أخرى في مجال التوقيع الإلكتروني**».

- بالرجوع لأحكام المادة (8-8) من القانون (2000-03)، نجدها تعرف موفر الخدمات في مجال المواصلات السلكية واللاسلكية بأنه: «**موفر خدمات: كل شخص معنوي أو طبيعي يقدم خدمات مستعملا وسائل المواصلات السلكية واللاسلكية**».

من خلال الجمع بين هذين العنصرين، يمكن أن نعرف مؤدي خدمات التصديق الإلكتروني بأنه كل شخص طبيعي أو معنوي يقدم خدمات مستعملا وسائل الاتصالات السلكية واللاسلكية، ويسلم شهادات إلكترونية أو يقدم خدمات أخرى في مجال التوقيع الإلكتروني.

أما في النص القانوني الثاني فقد كان من خلال القانون (15-04) المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، حيث ميز في المادة (2) منه بين نوعين من موفري الخدمات، فسمى النوع الأول ب "**الطرف الثالث الموثوق**" حسب المادة (11/2) بأنه: «**...الطرف الثالث الموثوق: شخص معنوي يقوم بمنح شهادات تصديق الكتروني موصوفة وقد يقدم خدمات أخرى متعلقة بالتصديق الإلكتروني لفائدة المتدخلين في الفرع الحكومي**».

---

(1)- مرسوم تنفيذي رقم 07-162 مؤرخ في 30 ماي 2007، يتعلق بنظام الاستغلال المطبق على كل أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية، ج.ر. ع 37 صادر في 07 جويلية 2007، يعدل ويتمم المرسوم التنفيذي رقـــم 01- 123 مؤرخ في 09 ماي 2001، ج.ر.ع 27 صادر في 13 ماي 2007.

أما النوع الثاني من موفري الخدمات؛ فقد سماه بـ: "**مؤدي خدمات التصديق الإلكتروني**"، والذي عرفه بموجب نص المادة (12/2) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين، بأنه: «...**مؤدي خدمات التصديق الإلكتروني: شخص طبيعي أو معنوي يقوم بمنح شهادات تصديق إلكتروني موصوفة، وقد يقدم خدمات أخرى في مجال التصديق الإلكتروني**».

من خلال هذين النصين يتبين لنا أن الطرف الثالث الموثوق عبارة عن شخص معنوي فقط، تنحصر مهامه في تقديم شهادات تصديق إلكتروني موصوفة وخدمات أخرى في مجال التصديق للمتدخلين في الفرع الحكومي، والمقصود بهم وفقا للمادة (13/2) من القانون نفسه، المتدخلون في الفرع الحكومي:«...**المؤسسات والإدارات العمومية والهيئات العمومية المحددة في التشريع المعمول به، والمؤسسات الوطنية المستقلة وسلطات الضبط، والمتدخلون في المبادلات ما بين البنوك، وكذا كل شخص أو كيان ينتمي إلى الفرع الحكومي بحكم طبيعته أو مهامه**».[1]

في حين أن مؤدي خدمات التصديق الإلكتروني يمكن أن يكون شخص طبيعي أو معنوي، إلا أن الفرق بينه وبين الطرف الثالث الموثوق، هو أن هذا الأخير يقدم خدماته للمتدخلين في الفرع الحكومي، بينما يقدم مؤدي خدمات التصديق الإلكتروني خدماته للأشخاص العادية فقط.

ما نلاحظه كذلك أن المشرع الجزائري ونظرا لحساسيته اتجاه المحررات الرسمية الإلكترونية والتي كنا قد بيناها سابقا، لجأ إلى وضع نظام قانوني خاص بالمكلفين بتقديم خدمات التصديق الإلكتروني في المجال الحكومي والذي أطلق عليه مصطلح الطرف الثالث

---

(1)- * **المؤسسات والإدارات العمومية:** الولاية، البلدية...

* **الهيئات العمومية:** مثل المستشفى، الجامعة...

* **المؤسسات الوطنية المستقلة:** مثل CNAS، CASNOS...

* **سلطات الضبط:** مثل البريد والمواصلات.

* **المتدخلون في المبادلات ما بين البنوك:** يقصد بها كل البنوك ما عدا البنك المركزي.

الموثوق، ذلك راجع إلى أن المتدخلين في الفرع الحكومي، عادة ما تصدر عنهم محررات إلكترونية رسمية تتسم بالحساسية، وتتعلق باستقرار وأمن البلد، وقد تتضمن سـرا من أسـرار الدولـة، وهو ما يتنافى مع إسناد مهمة إصدار شهادات تصديق إلكترونية لشخـص طبيعي أو معنوي، دون إخضاعها لنص قانوني يتسم بالحزم والصرامة، تختلف عن مزود الخدمات الذي يصدر شهادات تصديق موصوفة للأشخاص العادية.

نستخلص من كل التعاريف السابقة، أن مؤدي خدمات التصديق الإلكتروني هو طرف أجنبي عن العلاقة التعاقدية، يمكن أن يكون شخص طبيعي أو معنوي، يقوم بدور الوسيط الضامن لسلامة وسرية البيانات التي يتلقاها منهم، ويعمل على ترسيخ الثقة فيما بين المتعاملين، وذلك من خلال إصدار شهادات تصديق إلكترونية لكل متعامل يشهد بموجبها بصحة المعلومات والبيانات الواردة فيها، وبالتالي يحقق الأمن المعلوماتي للأطراف.

الفرع الثاني
نظام ترخيص وتفويض جهات التصديق الإلكتروني

فرضت أغلب التشريعات الحديثة ضوابط معينة لتنظيم عمل مؤدي خدمات التصديق الإلكتروني، فبينما ترى التشريعات العربية بضرورة إخضاع مزاولة خدمات التصديق الإلكتروني للترخيص المسبق من قبل الدولة وأن تكون محكومة بنظام تسجيل وموافقة على مزاولة عملها **(أولا)**، ترى تشريعات الإتحاد الأوروبي بضرورة عدم إخضاع هذا النشاط لأي ترخيص مسبـق، وإنما تركه لأسس المنافسة في السوق؛ بحيث تقوم هذه الجهات بتوريد خدماتها دون أن تحكمها شروط معينة أو تعليمات خاصة، مما ينعكس إيجابا على مستوى وجودة الخدمات المقدمة، غير أنه يمكن للدولة أن تنص على وجود تفويض للممارسة مهنة التصديق الإلكتروني **(ثانيا)**.

أولا: الترخيص للممارسة مهنة التصديق الإلكتروني

أخضعت التشريعات العربية مزاولة خدمات التصديق الإلكتروني للترخيص المسبق من قبل الهيئة المختصة، فمثلا نجد أن القانون التونسي قد نص من خلال (الفصل 8) من القانون

(83 لسنة 2000) المتعلق بالمبادلات والتجارة الإلكترونية، على إنشاء الوكالة الوطنية للمصادقة الإلكترونية [1]، وتعتبر الهيئة المخولة قانونا بمنح التراخيص لمزود خدمات التصديق الإلكتروني لمزاولة نشاطه.

تتولى هذه الهيئة وفق (الفصل 9) من قانون المبادلات والتجارة الإلكترونية التونسي، منح ترخيص تعاطي نشاط مزود خدمات المصادقة الإلكترونية على كامل تراب الجمهورية التونسية، السهر على مراقبة احترام مزود خدمات المصادقة الإلكترونية لأحكام هذا القانون ونصوصه التطبيقية، تحديد مواصفات منظومة إحداث الإمضاء والتدقيق، إبرام اتفاقات الاعتراف المتبادل مع الأطراف الأجنبية، وتساهم في أنشطة البحث والتكوين والدراسة ذات العلاقة بالمبادلات والتجارة الإلكترونية، كما تقوم بإصدار وتسليم وحفظ شهادات المصادقة الإلكترونية الخاصة بالأعوان العمومين المؤهلين للقيام بالمبادلات الإلكترونية، وبصفة عامة تقوم بكل نشاط آخر يقع تكليفها به من قبل سلطة الإشراف وله علاقة بميدان تدخلها.

كما مكّن المشرع التونسي الوكالة الوطنية للمصادقة الإلكترونية في ظل مهامها المتعلقة بالتدقيق، أن تدخل بصفة دورية إلى أي محل لمزود خدمات التصديق الإلكتروني قصد مراقبة الموزعات المستعملة لتوفير الخدمة، وكذا التدقيق في موثوقية المعدات ومدى مطابقة توفير الخدمة لكراس الشروط وفقا لما نص عليه الفصلين 21 و22 من الأمر عدد (1667 لسنة 2001) المتعلق بالمصادقة على دفتر الشروط الخاص بممارسة نشاط مزود خدمات المصادقة الإلكترونية [2].

---

(1)- ينص الفصل (8) من القانون (83 لسنة 2000) على: **«أحدثت مؤسسة عمومية لا تكتسي صبغة إدارية تتمتع بالشخصية المعنوية وبالاستقلال المالي أطلق عليها اسم " الوكالة الوطنية للمصادقة الإلكترونية" وتخضع في علاقتها مع الغير إلى التشريع التجاري، ومقرها بتونس العاصمة»**

(2)- أمر عدد 1667 لسنة 2001 مؤرخ في 17 جويلية 2001 يتعلق بالمصادقة على كراس الشروط الخاص بممارسة نشاط مزود خدمات المصادقة الإلكترونية. http://www.legislation.tn

ينص الفصل 21 من الأمر 1667 لسنة 2001 على أنه: **«يتعين على مزود خدمات المصادقة الإلكترونية تمكين الوكالة الوطنية للمصادقة الإلكترونية من دخول المحل ومراقبة الموزعات المستعملة لتوفير الخدمة والاطلاع على جميع الوثائق والملفات عند الاقتضاء»**؛ وينص الفصل 22 من الأمر نفسه على أن: **«تتولى الوكالة الوطنية للمصادقة الإلكترونية**

أما عن المشرع المصري فقد أنشأ بموجب المادة (2) من القانون (15 لسنة 2004) المتعلق بالتوقيع الإلكتروني، "هيئة تنمية صناعة تكنولوجيا المعلومات" "ITIDA"[1]، تتمتع بالشخصية الاعتبارية العامة وتتبع الوزير المختص، وتقوم بمباشرة مهامها المتعلقة بإصدار وتجديد التراخيص اللازمة لمزاولة أنشطة خدمات التوقيع الإلكتروني وفقا لأحكام القوانين واللوائح المنظمة لها، وغيرها من المهام التي نصت عليها المادة (4) [2] من القانون نفسه.

في حين نصت المادة (19) من القانون (15 لسنة 2004) سالف الذكر، على أنه لا يجوز مزاولة نشاط إصدار شهادة التصديق الإلكتروني إلا بترخيص من الهيئة، وذلك نظير مقابل يحدده مجلس إدارتها.

= التدقيق في موثوقية المعدات والقواعد المعتمدة ومطابقة توفير الخدمة لكراس الشروط ولإجراءات السلامة التي تم تقديمها في ملف مطلب الترخيص

ويشمل التدقيق عمليات قبول مطلب الشهادة وإصدارها وأنظمة النفاذ إلى المعلومات السرية.

ويمكن للوكالة أن تطالب مزود خدمات المصادقة الإلكترونية بتقديم جميع الإرشادات وأن تجري جميع الأبحاث على عين المكان وذلك مع المطالبة بتقديم الدفاتر الحسابية والعقود وبصفة عامة جميع الوثائق التي تراها ضرورية لأداء مهمتها.

تتم أعمال التدقيق بصفة دورية وكلما رأت الوكالة الوطنية للمصادقة الإلكترونية فائدة في ذلك»

(1)- ITIDA : **I**nformation **T**echnology **I**ndustry **D**evelopment **A**gency.

(2)- تنص المادة (4) من القانون (15 لسنة 2004) المتعلق بالتوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات المصري على أن: «**تباشر الهيئة الاختصاصات اللازمة لتحقيق أغراضها على الأخص ما يأتي:**

أ- إصدار وتجديد التراخيص اللازمة لمزاولة أنشطة خدمات التوقيع الإلكتروني وغيرها من الأنشطة في مجال المعاملات الإلكترونية وصناعة تكنولوجيا المعلومات، وذلك وفقا لأحكام القوانين واللوائح المنظمة لها؛

ب- تحديد معايير منظومة التوقيع الإلكتروني بما يؤدي إلى ضبط مواصفاتها الفنية؛

ج- تلقي الشكاوى المتعلقة بأنشطة التوقيع الإلكتروني والمعاملات الإلكترونية وتكنولوجيا المعلومات واتخاذ ما يلزم من شأنها؛

د- تقييم الجهات العاملة في مجال أنشطة تكنولوجيا المعلومات وتحديد مستوياتها الفنية بحسب نتائج هذا التقييم؛

هـ- تقديم المشورة الفنية بشأن المنازعات التي تنشأ بين الأطراف المعنية بأنشطة التوقيع الإلكتروني والمعاملات الإلكترونية وتكنولوجيا المعلومات؛

و- تقديم المشورة الفنية إلى الجهات العاملة في أنشطة تكنولوجيا المعلومات، وتدريب العاملين فيها؛

ز- إقامة المعارض والمؤتمرات والندوات المتخصصة في مجال تكنولوجيا المعلومات والاتصالات داخليا وخارجيا؛

- إنشاء الشركات التي تساعد في تنمية صناعة تكنولوجيا المعلومات والاتصالات أو المساهمة فيها؛

ط- إيداع وقيد وتسجيل النسخ الأصلية لبرامج الحاسب الآلي وقواعد البيانات، التي تتقدم بها الجهات أو الأفراد الناشرون والطابعون والمنتجون لها للمحافظة على حقوق الملكية الفكرية وغيرها من الحقوق».

في حين اشترط المشرع المغربي على مقدم خدمات المصادقة الإلكترونية الحصول على رخصة إدارية من قبل السلطة الوطنية المكلفة باعتماد ومراقبة المصادقة الإلكترونية، والتي عُهد إليها باقتراح معايير نظام الاعتماد على الحكومة، واتخاذ التدابير اللازمة لتفعيله، واعتماد مقدمي خدمات المصادقة الإلكترونية ومراقبة نشاطهم وفقا لما نصت عليه المادة (15) [1] من القانون (05-53) المتعلق بالتبادل الإلكتروني للمعطيات القانونية.

وتقوم السلطة الوطنية المكلفة باعتماد ومراقبة المصادقة الإلكترونية، في حالة اعتمادها لمقدم خدمة المصادقة الإلكترونية بنشر مستخرج من قرار الاعتماد في الجريدة الرسمية، وبمسك سجل بأسماء مقدمي خدمات المصادقة الإلكترونية المعتمدين، ينشر في نهاية كل سنة بالجريدة الرسمية [2].

كما تتأكد السلطة الوطنية المكلفة باعتماد ومراقبة المصادقة الإلكترونية من احترام مقدمي خدمات المصادقة الإلكترونية الذين يسلمون شهادات إلكترونية مؤمنة للالتزامات المنصوص عليها في أحكام القانون رقم (05-53) المتعلق بالتبادل الإلكتروني للمعطيات القانونية والنصوص المتخذة لتطبيقه [3].

ويجوز للسلطة الوطنية المكلفة اعتماد ومراقبة المصادقة الإلكترونية إما تلقائيا وإما بطلب من أي شخص يهمه الأمر، القيام بالتحقق أو طلب القيام بالتحقق من مطابقة نشاط مقدم خدمات المصادقة الإلكترونية الذي يسلم شهادة إلكترونية مؤمنة لأحكام القانون السالف الذكر، بل ويمكنها أن تستعين بخبراء لإنجاز مهامها المتعلقة بالمراقبة [4].

---

(1)- تنص المادة 15 من القانون 05-53 المتعلق بالتبادل الإلكتروني للمعطيات القانونية على أنه: «**يعهد إلى السلطة الوطنية المكلفة باعتماد ومراقبة المصادقة الإلكترونية المسماة بعده السلطة الوطنية، علاوة على المهام المسندة إليها بموجب مواد أخرى من هذا القانون، بالمهام التالية:**

- اقترا معايير نظام الاعتماد على الحكومة واتخاذ التدابير اللازمة لتفعيله؛

- اعتماد مقدمي خدمات المصادقة الإلكترونية ومراقبة نشاطهم»

(2)- أنظر المادة (16) من القانون 05-53 المتعلق بالتبادل الإلكتروني للمعطيات القانونية، مرجع سابق.

(3)- أنظر المادة (17) من القانون 05-53 المتعلق بالتبادل الإلكتروني للمعطيات القانونية، مرجع سابق.

(4)- أنظر المادة (18) من القانون 05-53 المتعلق بالتبادل الإلكتروني للمعطيات القانونية، مرجع سابق.

يُخول أعوان السلطة الوطنية، والخبراء المعينون من قبلها خلال ممارسة مهمة التحقق المكلفين بها، بعد إثبات صفاتهم، حق الولوج لأي مؤسسة والاطلاع على كل الآليات والوسائل التقنية المتعلقة بخدمات المصادقة الإلكترونية المؤمنة التي يعتبرونها مفيدة أو ضرورية لإنجاز مهمتهم [1].

اشترط قانون المعاملات الإلكترونية الأردني (15 لسنة 2015) من خلال المادة (26) منه على ضرورة الحصول على ترخيص لمزاولة نشاط التوثيق الإلكتروني، وفي حال مخالفة ذلك يعرض صاحبه لعقوبات مالية[2]، وأناط المشرع الأردني مهمة منح ترخيص مزاولة نشاط جهات التوثيق الإلكتروني لهيئة تنظيم قطاع الاتصالات باعتبارها الجهة المختصة باعتماد وبترخيص جهات التوثيق الإلكترونية وفقا لما تنص عليه المادة (23/ب)[3] من قانون المعاملات الإلكترونية، في حين أوكل المشرع الأردني مجلس الوزراء مهمة إصدار الأنظمة اللازمة لتنفيذ أحكام قانون المعاملات الإلكترونية بما في ذلك نظام الترخيص طبقا للمادة(27)[4] منه.

أما عن المشرع الجزائري فقد نص على مجموعة من الشروط المتعلقة بمزاولة خدمات التصديق الإلكتروني والتي تجعل من مؤدي خدمات التصديق الإلكتروني جديرا بالثقة، كما أنه ميز بين الطرف الثالث الموثوق ومؤدي خدمات التصديق الإلكتروني، فأخضع هذا الأخير

---

(1)- أنظر المادة (19) من القانون 05-53 المتعلق بالتبادل الإلكتروني للمعطيات القانونية، مرجع سابق.

(2)- تنص المادة (26) من قانون المعاملات الإلكترونية (15 لسنة 2015) على أنه: **«يعاقب كب من يمارس نشاط جهات التوثيق الإلكتروني داخل المملكة، دون الحصول على ترخيص أو اعتماد وفقا لأحكام هذا القانون والأنظمة الصادرة بمقتضاه بغرامة لا تقل عن (50000) خمسين ألف دينار ولا تزيد على (100000) مائة ألف دينار».**

(3)- تنص المادة (23/ب) من قانون المعاملات الإلكترونية (15 لسنة 2015) على أن: «... **ب- تكون هيئة تنظيم قطاع الاتصالات الجهة المختصة بترخيص جهات التوثيق الإلكتروني واعتمادها وتنظيم أعمالها وفقا للأنظمة والتعليمات التي تصدر بموجب أحكام هذا القانون».**

(4)- تنص المادة (27) من قانون المعاملات الإلكترونية (15 لسنة 2015) على أن: **«يصدر مجلس الوزراء الأنظمة اللازمة لتنفيذ أحكام هذا القانون بما في ذلك نظام ترخيص جهات التوثيق الإلكتروني واعتمادها والرسوم الواجب استفاؤها».**

وحده لنظام الترخيص لأجل مزاولة نشاطه دون الأول، ولأجل ذلك أوجد عدّة سلطات تساهم بشكل مباشر في عمل مؤدي خدمات التصديق الإلكتروني.

تم إنشاء هذه السلطات بموجب القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين، وقد أدرجها هذا القانون في الفصل الثاني من الباب الثالث تحت تسمية سلطات التصديق الإلكتروني، إذ تم إنشاء "**السلطة الوطنية للتصديق الإلكتروني**" بموجب المادة (16) من القانون نفسه لدى الوزير الأول كسلطة رئيسية إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، يطلق عليها في صلب النص مصطلح "**السلطة**"[1]، كما أصدر لمشرع الجزائري المرسوم التنفيذي رقم (16- 134) [2] الذي نظم بواسطته المصالح التقنية والإدارية للسلطة الوطنية للتصديق الإلكتروني وسيرها ومهامها.

تكلف "السلطة" بترقية استعمال التوقيع والتصديق الإلكترونيين، وتطويرهما وضمان موثوقية استعمالهما، وبإعداد سياستها المتعلقة بالتصديق الإلكتروني والسهر على تطبيقها، بعد الحصول على الرأي الإيجابي " **للهيئة المكلفة بالمراقبة**"، كما تقوم السلطة بالموافقة على سياسات التصديق الإلكتروني الصادرة عن " **السلطتين الفرعيتين الحكومية والاقتصادية للتصديق الإلكتروني**" وإبرام اتفاقيات الاعتراف المتبادل على المستوى الدولي، والمساهمة في اقتراح مشاريع تمهيدية للنصوص التشريعية أو التنظيمية ذات الصلة بالتوقيع الإلكتروني أو التصديق الإلكتروني على الوزير الأول، كما تقوم بعمليات التدقيق على مستوى السلطتين "**الحكومية والاقتصادية**" عن طريق" **الهيئة الحكومية المكلفة بالتدقيق**"[3].

ويتفرع عن "**السلطة**" كل من "**السلطة الحكومية للتصديق الإلكتروني**" التي تم إنشاؤها بموجب المادة (26) من القانون نفسه، إذ تنص هذه المادة على أنه: «**تنشأ لدى الوزير المكلف بالبريد وتكنولوجيات الإعلام والاتصال سلطة حكومية للتصديق الإلكتروني تتمتع**

---

(1)- أنظر المادة (16) من القانون (15- 04) المتعلق بالتوقيع والتصديق الإلكترونيين، مرجع سابق.

(2)- **مرسوم تنفيذي 16- 134** مؤرخ في 17 رجب 1437 الموافق ل 25 أفريل 2016، يحدد تنظيم المصالح التقنية والإدارية للسلطة الوطنية للتصديق الإلكتروني وسيرها ومهامها ج. ر.ع، 26 صادر بتاريخ 28 أفريل 2016.

(3)- نصت على هذه المهام المادة (8) من القانون 15- 04، (ق. ت. ت. إ).

بالاستقلال المالي والشخصية المعنوية»، وجاء المرسوم التنفيذي رقم (16- 135) [1] الذي حدد طبيعة السلطة الحكومية للتصديق الإلكتروني وتشكيلها وتنظيمها وسيرها، وكيفها على أنها سلطة إدارية تتمتع بالشخصية المعنوية والاستقلال المالي، تكلف بالمهام المتعلقة بمتابعة ومراقبة نشاط التصديق الإلكتروني للأطراف الثلاثة الموثوقة، مع توفير خدمات التصديق الإلكتروني لفائدة المتدخلين في الفرع الحكومي[2].

ويتفرع عنها أيضا "السلطة الاقتصادية للتصديق الإلكتروني" التي أنشأت بموجب المادة (29) من القانون (15-04) سالف الذكر، والتي تنص على أنه: **«تُعيَن السلطة المكلفة بضبط البريد والمواصلات السلكية واللاسلكية [3] في مفهوم هذا القانون، سلطة اقتصادية**

---

(1)- مرسوم تنفيذي رقم 16- 135 مؤرخ في 17 رجب 1437 الموافق ل 25 أفريل 2016، يحدد طبيعة السلطة الحكومية للتصديق الإلكتروني وتشكيلها وتنظيمها وسيرها، ج. ر. ع، 26. صادر بتاريخ 28 أفريل 2016.

(2)- أنظر المادة (28) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين، سالف الذكر.

(3)- خلال سنة 2001 قامت الجزائر بإنشاء هيئة مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي أطلق عليها اسم "**سلطة الضبط للبريد والاتصالات السلكية واللاسلكية**" **Autorité de Régulation de la Poste et de Télécommunication**"

أو ما يطلق عليها اختصار " **ARPT** " تتولى السهر على تنفيذ التوجيهات الوطنية في مجال تكنولوجيا الإعلام والاتصال، وقد كلفت هذه الهيئة بتطبيق خطط الدولة المعلنة لتحرير سوق البريد والاتصالات وانفتاحه على المنافسة، وجذب الاستثمارات إليه وحماية حقوق المستهلكين.

وتم إنشاء هذا الجهاز التنظيمي بموجب القانون رقم (2000- 03) المؤرخ في 05 أوت 2000 والذي يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، ج.ر.ع 48، والذي يمنح لهذه الهيئة الصلاحيات الكفيلة بالضبط والمراقبة والمتابعة المتعلقة بهذا السوق، وحددت المادة 13 من الفصل الثالث لهذا القانون مهام ووظائف سلطة الضبط كالآتي:

1- منح رخص الاستغلال لمتعاملي الهاتف النقال والثابت، وموفري خدمات الانترنت ومراكز النداء... مع وضع دفتر شروط موحد يحدد المواصفات والمقاييس الواجب توفرها في المتعاملين، والقواعد المطبقة عليهم، مع محاولة تحقيق المساواة بينهم.

2- إعادة هيكلة قطاع البريد والمواصلات السلكية واللاسلكية من خلال توفير بيئة تنافسية فعالة بين مختلف متعاملي هذا القطاع.

3- التهيئة الرقمية لتقديم خدمات تكنولوجيا الإعلام والاتصال ذات جودة، وضمانها في شروط موضوعية وشفافة، وغير تمييزية، مشجعة لانضمام الجميع في مختلف أقاليم الوطن إلى المجمع المعلوماتي.

4- مواكبة الثورة التكنولوجية الجديدة وعدم التأخر عما يجري، والسعي للتعاون والتنسيق مع مختلف الهيئات الدولية والوطنية، بغية اقتراح كل ما من شانه النهوض بهذا القطاع. =

للتصديق الإلكتروني»، مكلفة بمتابعة ورقابة مؤدي خدمات التصديق الإلكتروني، وبإعداد سياسة التصديق الخاصة بها وعرضها على "السلطة" والسهر على تطبيقها، ومنح التراخيص لمؤدي خدمات التصديق الإلكتروني بعد موافقة "السلطة الوطنية للتصديق الإلكتروني"[1].

وعليه؛ يخضع نشاط تأدية خدمات التصديق الإلكتروني في الجزائر إلى ترخيص تمنحه "السلطة الاقتصادية للتصديق الإلكتروني" وفقا لما تنص عليه المادة (33) من القانون (15- 04) سالف الذكر، وتشترط المادة (35) من القانون نفسه ضرورة أن يحصل الطالب على شهادة التأهيل قبل الحصول على الترخيص، تهدف هذه الشهادة إلى تهيئة جميع الوسائل اللازمة للقيام بخدمات التصديق الإلكتروني، وتمنح لكل شخص طبيعي أو معنوي لمدة سنة واحدة قابلة للتجديد مرّة واحدة.

تبلغ شهادة التأهيل للمعني في أجل أقصاه (60) يوم من تاريخ استلام الطلب المثبت بإشعار بالاستلام[2]، وفي حال رفض منح شهادة التأهيل، وجب أن يكون الرفض مسببا، ويتم تبليغه مقابل إشعار بالاستلام [3]، ذلك لتمكين طالب شهادة التصديق من الطعن في هذا القرار أمام السلطة في أجل شهر واحد من تاريخ تبليغه وفق ما تنص عليه المادة (31) من القانون (15- 04) المتعلق بالتوقيع والتصديق الإلكترونيين السالف الذكر.

بعد حصول مؤدي خدمات التصديق الإلكتروني على شهادة التأهيل، تصدر السلطة الاقتصادية وفقا لنص المادة (40) من القانون (15- 04) أعلاه، قرارا مسببا بمنح الترخيص مدة صلاحيته (05) سنوات قابلة للتجديد عند انتهاء المدة، وفقا للشروط المحددة في دفتر الأعباء، الذي يحدد شروط وكيفيات تأدية خدمات التصديق الإلكتروني[4]، بحيث يبلّغ هذا

5- سلطة الضبط هي الهيئة المخولة قانونا باتخاذ القرارات الزجرية والعقابية كفرض الغرامات، وسحب الرخص من المتعاملين في حالة مخالفة القوانين المؤطرة للسوق.

6- القيام بمهمة التحكيم لفض النزاعات الناشئة بين المتعاملين بعضهم مع بعض أو مع المستعملين.

(1)- أنظر المادة (30) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين، مرجع سابق.

(2)- أنظر المادة (35 ف 2) من القانون 15- 04 المتعلق بالتوقيع والتصديق الإلكترونيين، مرجع سابق.

(3)- أنظر المادة (37) من القانون 15- 04 المتعلق بالتوقيع والتصديق الإلكترونيين، مرجع سابق.

(4)- أنظر المادة (40) من القانون 15- 04 المتعلق بالتوقيع والتصديق الإلكترونيين، مرجع سابق.

القرار لصاحب شهادة التأهيل بصفة شخصية، وهو غير قابل للتنازل عنه للغير[1]، في أجل (60) يوم من تاريخ استلام الطلب المثبت بوصل إشعار بالاستلام، وذلك مقابل مبلغ مالي تحدد قيمته عن طريق التنظيم، وفقا لنص المادة (36) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين.

أثناء مدة الترخيص، أي أثناء مزاولة مؤدي خدمات التصديق الإلكتروني لمهامه يخضع لمراقبات فجائية وعمليات تدقيق دورية من قبل السلطة الاقتصادية، للتأكد من مدى التزام مؤدي خدمات التصديق الإلكتروني بما هو وارد في دفتر الأعباء المحدد لشروط وكيفيات تقديم خدمات التصديق الإلكتروني، وفقا لنص المادة (52) من القانون (15-04) سالف الذكر.

ثانيا: التفويض للممارسة مهنة التصديق الإلكتروني

على خلاف الدول العربية التي تتبع نظام الترخيص للقيام بمهمة مؤدي خدمات التصديق الإلكتروني، لا يخضع نشاط تأدية خدمات التصديق الإلكتروني لأي ترخيص مسبق في فرنسا، بل أبقت هذا النشاط مفتوح أمام الجميع لخلق نوع من التنافس، مما ينعكس إيجابا على مستوى وجودة الخدمات المقدمة. إلا أن ممارسة نشاط التصديق الإلكتروني في فرنسا يكون عن طريق اعتماد ممنوح من الهيئات المعينة من قبل وزير الصناعة الذي يحدد إجراءات اعتمادها وإجراءات تقييم وتأهيل مقدمي خدمات التصديق الإلكتروني، وبذلك لم يفرض المشرع الفرنسي أي ترخيص لممارسة عملية التصديق؛ وإنما يمنح صفة المؤهل[2].

وقد حددت المادة (1) من المرسوم (2002-535) [3] السلطة المخول لها ممارسة نشاط التصديق الالكتروني، وتتمثل في الإدارة المركزية لأمان أنظمة المعلومات، ويجوز لها منح التراخيص لمراكز التصديق التي تعتمدها.

---

(1)- أنظر المادة (39) من القانون 15- 04 المتعلق بالتوقيع والتصديق الإلكترونيين، مرجع سابق.

(2)- **كياري أسماء**، النظام القانوني لجهات التصديق الإلكتروني، مجلة القانون العام الجزائري والمقارن، المجلد 01، العدد 02، جامعة جيلالي اليابس، سيدي بلعباس، 2015، ص 67.

(3)- Décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information. JORF n 92 du 19 avril 2002p 6944.
www.legifrance.gouv.fr

كما صدر قرار في (31 ماي 2002) [1] ينص على أنه يتم اعتماد الهيئات التي يعهد لها مهمة تقييم مقدمي خدمات التصديق الالكتروني من قبل اللجنة الفرنسية للاعتماد، أو من الهيئات الموقعة على اتفاق أوروبي متعدد الأطراف يدخل ضمن التنظيم الأوروبي لهيئات الاعتماد.

وعليه؛ يتعين على مؤدي نشاط التصديق الإلكتروني الراغب في الحصول على الاعتماد أن يتقدم بطلب أمام الإدارة المركزية لأمان منظومة المعلومات[2]، ثم يقوم باختيار أحد مراكز التقييم المعتمدة من أجل إجراء تقييم لمنتجاته [3].

عندما ينهي مركز التقييم عمليات الفحص يقوم بإرسال تقرير إلى الإدارة المركزية لأمان أنظمة المعلومات[4]، ويتعين على هذه الأخيرة أن تُعد تقريرا خلال شهر يسمى بتقرير التصديق؛ فإما أن تُسلم شهادة لمؤدي الخدمات بمطابقة منتجاته وأنظمته لشروط الأمان أو أن ترفض التصديق[5].

---

(1)- Arrêt du 31 mai 2002 relatif à la reconnaissances de la qualification des prestataires de certification électronique et à l'accréditation des organismes chargés de l'évaluation, JORF n 132 du 08 juin 2002, p 10223. www.legifrance.gouv.fr.

(2)- :Art 2 du Décret n° 2002-535 **:« Une évaluation en vue de la certification prévue à l'article 1er est effectuée à la demande d'un commanditaire qui adresse à la direction centrale de la sécurité des systèmes d'information un dossier d'évaluation. Le dossier comporte notamment la description du système de sécurité à évaluer, les dispositions prévues pour lui conférer sa pleine efficacité ainsi que le programme de travail prévisionnel permettant une évaluation.**
Dès réception de ce dossier, la direction centrale de la sécurité des systèmes d'information si elle estime que les objectifs de sécurité ne sont pas définis de manière pertinente au regard des normes, prescriptions techniques ou règles de bonne pratique applicables au moment où commence l'évaluation, notifie au commanditaire qu'elle ne pourra pas en l'état du dossier procéder à la certification envisagée».

(3)- Art 3 du Décret n° 2002-535**: «Le commanditaire de l'évaluation choisit un ou plusieurs centres d'évaluation, agréés dans les conditions prévues au chapitre II, pour procéder à celle-ci. Avant le début des travaux, il détermine avec chacun de ces centres :**
a) Le produit ou le système à évaluer ainsi que les objectifs de sécurité ;
b) Les conditions de protection de la confidentialité des informations qui seront traitées dans le cadre de l'évaluation
c) Le coût et les modalités de paiement de l'évaluation ;
d) Le programme de travail et les délais prévus pour l'évaluation.
Le commanditaire est tenu d'assurer la mise à la disposition des centres d'évaluation qu'il a choisis et de la direction centrale de la sécurité des systèmes d'information, si elle en fait la demande, de tous les éléments nécessaires au bon accomplissement de leurs travaux, le cas échéant après accord des fabricants concernés ».

(4)- Art 6 du Décret n° 2002-535**: «Au terme des travaux d'évaluation, chaque centre remet un rapport d'évaluation au commanditaire et à la direction centrale de la sécurité des systèmes d'information. Ce rapport est un document confidentiel dont les informations sont couvertes par le secret industriel et commercial ».**

(5)- Art 7 du Décret n° 2002-535: **«Le commanditaire et la direction centrale de la sécurité des systèmes d'information valident les rapports d'évaluation en liaison avec le centre d'évaluation intervenant. Lorsque=**

تصدر هذه الشهادة من قبل الوزير الأول صالحة لمدة سنتين، تشهد بأن منتجات وأنظمة المعلومات الخاضعة للتقييم تستوفي خصائص الأمان، وأن التقييم كان طبقا للقواعد والمعايير السارية المفعول[1].

الفرع الثالث

شروط ممارسة نشاط مؤدي خدمات التصديق الإلكتروني

نظرا لخطورة وأهمية الدور المسند لجهات التصديق الإلكتروني في تحقيق عنصري الثقة والأمان في المعاملات الإلكترونية، نصت مختلف التشريعات المنظمة للمعاملات الإلكترونية على مجموعة من الشروط والمتطلبات الأساسية لتتمكن من ممارسة مهامها ووظائفها.

إذ نص قانون اليونسترال النموذجي لسنة (2001) الخاص بالتوقيعات الإلكترونية من خلال المادتين (9) و(10) على مجموعة من الشروط الفنية والتقنية لمزاول نشاط مؤدي خدمات التصديق الإلكتروني، تتمثل أساسا في ضرورة اعتماده على موظفين يتمتعون بالقدرة والمعرفة خصوصا فيما يتعلق بميدان تكنولوجيا الإعلام والاتصال، إضافة إلى توافره على موارد مالية من شأنها أن تساهم في تغطية مختلف الأضرار، وأن يستخدم معدات وبرامج حديثة مرتبطة بنظام شبكي مؤمن بنظم أمن معلومات، وغيرها من الشروط التقنية [2]. كما نص عليها

=l'ensemble des rapports prévus a été validé, la direction centrale de la sécurité des systèmes d'information élabore un rapport de certification dans un délai d'un mois. Ce rapport, qui précise les caractéristiques des objectifs de sécurité proposés, conclut soit à la délivrance d'un certificat, soit au refus de la certification. Le rapport de certification peut comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Il est, au choix du commanditaire, communiqué ou non à des tiers ou rendu public.

(1)- Art 8 du Décret n° 2002-535: **«Le certificat est délivré par le Premier ministre». Il atteste que l'exemplaire du produit ou du système soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Il atteste également que l'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises ».**

وللمزيد من التفاصيل حول كيفية اعتماد نشاط مؤدي خدمات التصديق الإلكتروني بفرنسا راجع كل من: **دحماني سمير**، التوثيق في المعاملات الإلكترونية (دراسة مقارنة)، مذكرة لنيل شهادة الماجستير في القانون، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، 2015، ص 64؛ **محمد رضا أزرو**، مرجع سابق، ص 250؛ **عيسى غسان ربضي**، مرجع سابق، ص 121.

(2)- أنظر المواد 9 و10 من قانون اليونسترال النموذجي بشأن التوقيعات الإلكترونية لسنة 2001، مرجع سابق.

كذلك التنظيم الأوروبي (910-2014) بموجب نص المادة (2/24)[1]، وكذا القانون الفرنسي بموجب المادة (1) من المرسوم (1416-2017).

---

(1)- Article 24/2 du le règlement n°910/2014 **:«…Un prestataire de services de confiance qualifié qui fournit des services de confiance qualifiés:**

a) informe l'organe de contrôle de toute modification dans la fourniture de ses services de confiance qualifiés et de son intention éventuelle de cesser ces activités;

b) emploie du personnel et, le cas échéant, des sous-traitants qui possèdent l'expertise, la fiabilité, l'expérience et les qualifications nécessaires, qui ont reçu une formation appropriée en ce qui concerne les= =règles en matière de sécurité et de protection des données à caractère personnel et appliquent des procédures administratives et de gestion correspondant à des normes européennes ou internationales;

c) en ce qui concerne le risque de responsabilité pour dommages conformément à l'article 13, maintient des ressources financières suffisantes et/ou contracte une assurance responsabilité appropriée, conformément au droit national;FR L 257/98 Journal officiel de l'Union européenne 28.8.2014

d) avant d'établir une relation contractuelle, informe, de manière claire et exhaustive, toute personne désireuse d'utiliser un service de confiance qualifié des conditions précises relatives à l'utilisation de ce service, y compris toute limite quant à son utilisation;

e) utilise des systèmes et des produits fiables qui sont protégés contre les modifications et assure la sécurité technique et la fiabilité des processus qu'ils prennent en charge;

f) utilise des systèmes fiables pour stocker les données qui lui sont fournies, sous une forme vérifiable de manière que:

i) les données ne soient publiquement disponibles pour des traitements qu'après avoir obtenu le consentement de la personne concernée par ces données;

ii) seules des personnes autorisées puissent introduire des données et modifier les données conservées;

iii) l'authenticité des données puisse être vérifiée;

g) prend des mesures appropriées contre la falsification et le vol de données;

h) enregistre et maintient accessibles pour une durée appropriée, y compris après que les activités du prestataire de services de confiance qualifié ont cessé, toutes les informations pertinentes concernant les données délivrées et reçues par le prestataire de services de confiance qualifié, aux fins notamment de pouvoir fournir des preuves en justice et aux fins d'assurer la continuité du service. Ces enregistrements peuvent être effectués par voie électronique;

i) a un plan actualisé d'arrêt d'activité afin d'assurer la continuité du service conformément aux dispositions vérifiées par l'organe de contrôle au titre de l'article 17, paragraphe 4, point i);

j) assure le traitement licite de données à caractère personnel conformément à la directive 95/46/CE;

k) au cas où le prestataire de services de confiance qualifié délivre des certificats qualifiés, établit et tient à jour une base de données relative aux certificats.

3. Lorsqu'un prestataire de services de confiance qualifié qui délivre des certificats qualifiés décide de révoquer un certificat, il enregistre cette révocation dans sa base de données relative aux certificats et publie le statut de révocation du certificat en temps utile, et en tout état de cause dans les vingt-quatre heures suivant la réception de la demande. Cette révocation devient effective immédiatement dès sa publication.

4. En ce qui concerne le paragraphe 3, les prestataires de services de confiance qualifiés qui délivrent des certificats qualifiés fournissent à toute partie utilisatrice des informations sur la validité ou le statut de révocation des certificats qualifiés qu'ils ont délivrés. Ces informations sont disponibles, au moins par certificat, à tout moment et au-delà de la période de validité du certificat, sous une forme automatisée qui est fiable, gratuite et efficace.

5. La Commission peut, au moyen d'actes d'exécution, déterminer les numéros de référence des normes applicables aux systèmes et produits fiables, qui satisfont aux exigences du paragraphe 2, points e) et f), du présent article. Les systèmes et les produits fiables sont présumés satisfaire aux exigences fixées au présent=

بينما حددها القانون التونسي بموجب الفصل (11) من القانون (83 لسنة2000) المتعلق بالمبادلات والتجارة الإلكترونية، حيث نص على ضرورة تمتع الشخص الراغب في تأدية خدمات التصديق الإلكتروني بالجنسية التونسية من خمس سنوات على الأقل، وأن يكون متحصلا على شهادة الأستاذية أو ما يعادلها، وأن يكون مقيما بتونس ومتمتعا بكافة حقوقه المدنية والسياسية، وأن لا يمارس أي نشاط مهني آخر.

أما عن المشرع المغربي فقد نص بموجب المادة (21 ف1و2) من القانون (05-53) المتعلق بالتبادل الإلكتروني للمعطيات القانونية، على أن: «**يشترط في طالب الاعتماد لاكتساب صفة مقدم خدمات المصادقة الإلكترونية أن يكون طالب الاعتماد مؤسسا في شكل شركة يوجد مقرها الاجتماعي بتراب المملكة وأن يكون:**

1- متوافرا على شروط تقنية تضمن:

أ- الوثوق بخدمات المصادقة الإلكترونية التي يقدمها، ولا سيما ما يتعلق بالسلامة التقنية والتشفيرية الخاصة بالوظائف التي تقوم بها نظم ووسائل التشفير المقترحة من لدنه؛

ب- سرية المعطيات المتعلقة بإنشاء التوقيع الإلكتروني التي يقدمها للموقع؛

ت- توافر مستخدمين لهم المؤهلات اللازمة لتقديم خدمات المصادقة الإلكترونية؛

ث- الإمكانية التي تتيح للشخص الذي سلمت إليه الشهادة قصد إلغائها في الحال وبكل يقين؛

ج- التحديد الدقيق لتاريخ وساعة تسليم الشهادة الإلكترونية وإلغائها؛

- وجود نظام للسلامة، قادر على اتقاء تزوير الشهادات الإلكترونية والتأكد من أن معطيات إنشاء التوقيع الإلكتروني تطابق معطيات التحقق منه عندما تقدم في آن واحد المعطيات معا؛

2- قادرا على المحافظة، عند الاقتضاء بشكل إلكتروني، على جميع المعلومات المتعلقة بالشهادة الإلكترونية التي قد تبدو ضرورية لإثبات التصديق الإلكتروني أمام القضاء، بشرط أن تضمن نظم المحافظة على الشهادات الإلكترونية:

أ- أن إدخال المعطيات وتغييرها لا يسمح بهما إلا للأشخاص المرخص لهم لهذا الغرض من لدن مقدم الخدمة؛

ب- أن اطلاع العموم على شهادة إلكترونية لا يتأتى دون موافقة سابقة من صاحب الشهادة؛

ت- أن بالإمكان كشف أي تغيير من شأنه أن يخل بسلامة النظام؛ ...»

=article lorsqu'ils respectent ces normes. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2».

وفي ذات السياق، نص المشرع المصري بموجب المادة (12)[1] من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري على المتطلبات الواجب توافرها لدى طالب الحصول على الترخيص لأجل ممارسة نشاط التصديق الإلكتروني، كما أضاف المشرع المصري من خلال المادة (14) من القانون نفسه، شرطا آخر يتعلق بالقدرة المالية لطالب الترخيص إذ تنص هذه المادة على ضرورة أن يقدم هذا الأخير الضمانات والتأمينات التي يحددها مجلس إدارة الهيئة

(1)- تنص المادة 12 من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري على أنه: «**يجب أن يتوافر لدى طالب الحصول على الترخيص بإصدار شهادات التصديق الإلكتروني المتطلبات التالية:**

أ – نظام تأمين المعلومات وحماية البيانات وخصوصيتها بمستوى حماية لا يقل عن المستوى المذكور في المعايير والقواعد المشار إليها في الفقرة (د) من الملحق الفني والتقني للائحة.

ب – دليل إرشادي يتضمن ما يلي:

1- إصدار شهادات التصديق الإلكتروني،

2- إدارة المفاتيح الشفرية،

3- إدارة الأعمال الداخلية،

4- إدارة التأمين والكوارث.

وذلك وفقا للمعايير الفنية والتقنية المذكورة في الفقرة (هـ) من الملحق الفني والتقني للائحة.

ج – منظومة تكوين بيانات إنشاء التوقيع الإلكتروني مؤمنة وفقا للضوابط الفنية والتقنية المنصوص عليها في المواد (2-3-4) من هذه اللائحة.

د – نظام لتحديد تاريخ ووقت إصدار الشهادات، وإيقافها، وتعليقها، وإعادة تشغيلها وإلغائها.

هـ – نظام للتحقق من الأشخاص المصدر لهم شهادات التصديق الإلكتروني، والتحقق من صفاتهم المميزة.

و – المتخصصون من ذوي الخبرة الحاصلين على المؤهلات الضرورية لأداء الخدمات المرخص بها.

ز – نظام حفظ بيانات إنشاء التوقيع الإلكتروني وشهادات التصديق الإلكتروني طوال المدة التي تحددها الهيئة في الترخيص، وتبعا لنوع الشهادة المصدرة. وذلك فيما عدا مفاتيح الشفرة الخاصة التي تصدرها للموقع فلا يتم حفظها إلا بناء على طلب من الموقع وبموجب عقد مستقل يتم إبرامه بين المرخص له والموقع ووفقا للقواعد الفنية والتقنية لحفظ هذه المفاتيح التي يضعها مجلس إدارة الهيئة.

ح – نظام للحفظ على السرية الكاملة للأعمال المتعلقة بالخدمات التي يرخص بها، وللبيانات الخاصة بالعملاء.

ط – نظام لإيقاف الشهادة في حالة ثبوت توافر حالة من الحالات الآتية:

1- العبث ببيانات الشهادة أو انتهاء مدة صلاحيتها.

2- سرقة أو فقد المفتا الشفري الخاص أو البطاقة الذكية، أو عند الشك في حدوث ذلك.

3- عدم التزام الشخص المصدر له شهادة التصديق الإلكتروني ببنود العقد البرم مع المرخص له.

ويكون نظام إيقاف الشهادات وفقا للقواعد والضوابط التي يضعها مجلس إدارة الهيئة».

لتغطية أي أضرار أو أخطار تتعلق بذوي الشأن، وذلك في حالة إنهـــاء الترخيـص لأي سبب، أو لأجل تغطية أي إخلال من جانبه لالتزاماته الواردة في الترخيص.

وفيما يخص المشرع الجزائري، فقد ألزم طالب الترخيص بموجب المادة (34)[1] من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين سالف الذكر، بمجموعة من الشروط الفنية والتقنية، كأن يكون خاضعا للقانون الجزائري بالنسبة للشخص المعنوي، أو الجنسية الجزائرية بالنسبة للشخص الطبيعـي، كما يجب أن يتمتع بقدرة ماليـة كافـية، وبمؤهلات وخبرة ثابتة في ميدان تكنولوجيات الإعلام والاتصال للشخص الطبيعي أو للمسير للشخص المعنوي، وأخيرا أن لا يكون قد سبق الحكم عليه في جناية أو جنحة تتنافى مع تأدية خدمات التصديق الإلكتروني.

عند مقارنة الشروط والمتطلبات التي نصت عليها تشريعات المعاملات الإلكترونية سالفة الذكر يظهر جليا قصور التشريع الجزائري في تحديد هذه الشروط، فعلى سبيل المثال الشرط المتعلق بالخبرة الفنية والتقنية، نجد أن المشرع الجزائري قد نص على ضرورة تمتع الشخص بمؤهلات ثابتة في مجال تكنولوجيات الإعلام والاتصال، إلا أن صياغة المادة جاءت عامة وغير مفصلة على عكس ما نص عليه كل من المشرع المغربي والمصري وكذا التنظيم الأوروبي، إذ تطرقت لهذه الحيثية بكثير من التفصيل وذلك لتنجب أي لبس أثناء تقييم هذه المؤهلات.

كذلك اشتراط المشرع الجزائري على طالب الترخيص تمتعه بقدرة مالية كافية دون تحديد لهذه القدرة، ولا على أي أساس يتم تقديرها مما ترك الأمر غامضا، على خلاف المشرع المصري الذي أوكل مهمة تحديد الضمانات والتأمينات لمجلس إدارة الهيئة لأجل تغطية أي أضرار أو أخطار.

---

(1)- تنص المادة (34) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين على أنه: «**يجب على كل طالب ترخيص لتأدية خدمة التصديق الإلكتروني أن يستوفي الشروط الآتية:**

- **أن يكون خاضعا للقانون الجزائري للشخص المعنوي أو الجنسية الجزائرية للشخص الطبيعي،**
- **أن يتمتع بقدرة مالية كافية،**
- **أن يتمتع بمؤهلات وخبرة ثابتة في ميدان تكنولوجيات الإعلام والاتصال للشخص الطبيعي أو المسير للشخص المعنوي،**
- **أن لا يكون قد سبق الحكم عليه في جناية أو جنحة تتنافى مع نشاط تأدية خدمات التصديق الإلكتروني».**

وعليه؛ نرى أنه يتعين على المشرع الجزائري إعادة صياغة المادة (34) من القانون (15-04) المتعلقة بتحديد الشروط والمتطلبات الفنية في طالب الترخيص لممارسة نشاط مؤدي خدمات التصديق الإلكتروني بشكل دقيق ومفصل؛ وذلك لتجنب أي لبس أثناء تطبيقها.

بيّنا من خلال ما سبق الإطار القانوني لممارسة نشاط التصديق الإلكتروني، فبمجرد توافرها في الشخص الراغب بممارسة نشاط مؤدي خدمات التصديق الإلكتروني تقع على عاتقه مجموعة من الالتزامات القانونية والتقنية وجب عليه احترامها، وأي إخلال بهذه الالتزامات تعرضه للمساءلة، وهذا ما سيتم توضيحه من خلال المبحث الموالي.

المبحث الثاني
الآثار القانونية المترتبة عن عملية التصديق الإلكتروني

إن الاعتراف التشريعي بالمحررات الإلكترونية؛ ومنحها الحجية ذاتها المقررة للمحررات التقليدية؛ يفرض شروط قانونية في التوقيع الإلكتروني تتلاءم والبيئة الإلكترونية، مع وجود آلية تحقق الثقة والأمان في التوقيع الإلكتروني تتمثل في جهات التصديق الإلكتروني، فطبيعة المعاملات الإلكترونية التي تتم في بيئة افتراضية فرضت ضرورة توفير قدر عال من الثقة والأمان لدى المتعاقدين، ذلك من خلال توفير الضمانات الكافية لتحديد هويـــة المتعـــاقدين والتأكد من طبيعة التعاقد ومضمونه.

ولتحقيق هذا الغرض كان لا بُدّ من اللجوء إلى أطراف محايدة قصد توثيق المعاملات الإلكترونية، وذلك عن طريق آلية التصديق الإلكتروني التي تعمل على خلق بيئة إلكترونية آمنة للتعامل عبر شبكة الانترنت، فمؤدي خدمات التصديق الإلكتروني يقوم بدور الوسيط المؤتمن بين المتعاملين في البيئة الإلكترونية. إذ يعمل على ضمان أمن المعاملات الإلكترونية، ويزيل مخاوف المتعاملين فيما يتعلق بإمكانية إطلاع الغير على مضمون البيانات الإلكترونية أو قرصنتها، كما يؤكّد هوية الأطراف المتعاقدة وصحة توقيعاتهم، وأن هذه التوقيعات لم تتعرض إلى أي عبث أو تلاعب أو تغيير؛ ذلك بإصدار شهادات تصديق إلكترونية تؤكد هوية الموقعين **(مطلب أول)**.

غير أنه قد يحدث أن يقصّر مؤدي خدمات التصديق الإلكتروني أثناء قيامهم بمهـــامهم؛ كأن يعتمدوا في إصدارهم لشهادات التصديق الإلكتروني على معلومات مغلوطة غير مطابقة للواقع، وأن لا يتم اكتشاف ذلك إلا بعد إتمام المعاملة اعتمادا على الشهادات غير الصحيحة، فتخل هذه الشهادات بالثقة المشروعة التي أولاها المتعاملون مع مؤدي خدمات التصديق الإلكتروني التي أصدروها، حينها تثار مسؤوليتهم تجاه من أصابهم ضرر إثر تعاملهم اعتمادا على هذه الشهادات غير الصحيحة **(مطلب ثان)**.

المطلب الأول

التزامات مؤدي خدمات التصديق الإلكتروني

بمجرد أن يتحصل مؤدي خدمات التصديق الإلكتروني على الترخيص من قبل الجهات الإدارية المختصة في الدولة لمزاولة نشاط التصديق الإلكتروني، تترتب على عاتقه مجموعة من الالتزامات تختلف طبيعتها بحسب مصدرها، فقد تكون مستمدة من التشريعات الخاصة بالمعاملات الإلكترونية، أو قد تكون أحكامها مُتَضّمنة في القواعد العامة لمختلف القوانين السارية.

أقرت تشريعات الإثبات الإلكتروني العديد من الالتزامات التي فرضتها على مؤدي خدمات التصديق الإلكتروني، وعلى الرغم من تنوعها وتعددها إلا أنه توجد التزامات مشتركة اتفقت عليها هذه التشريعات؛ أهمها تلك الالتزامات المتعلقة بحماية وتأمين المعلومات التي يجمعها مؤدي خدمات التصديق الإلكتروني والمتعلقة بأطراف المعاملات الإلكترونية **(فرع أول)**، وكذا الالتزامات التي تتعلق بكيفية إصدار شهادات التصديق الإلكتروني وإلغائها وتعليق العمل بها، على اعتبار هذا الالتزام من أهم الالتزامات التي تقع على عاتق مؤدي خدمات التصديق الإلكتروني **(فرع ثان)**.

الفرع الأول

الالتزامات المتعلقة بصحة وسرية البيانات الشخصية للموقع

تعتبر المعلومات والبيانات الخاصة بالموقع التي يتحصل عليها مؤدي خدمات التصديق الإلكتروني –سواء قدمها الموقع بنفسه أو جمعها مؤدي خدمات التصديق الإلكتروني من الغير– ذات أهمية كبيرة نظرا لطابعها الشخصي، لذا يتعين عليه في هذه الحالة أن يتحرى دقة وصحة هذه المعلومات أثناء جمعها **(أولا)**، وكذا أن يلتزم بالأحكام المتعلقة بحماية الأشخاص الطبيعيين عند معالجته لهذه المعلومات، وأن يحافظ على سريتها، كما لا يمكنه استعمال هذه المعلومات إلا في إطار نشاطه المتعلق بالتصديق الإلكتروني **(ثانيا)**.

أولا: الالتزام بالتحقق من صحة البيانات

يلتزم مؤدي خدمات التصديق الإلكتروني بالتحقق من صحة البيانات المقدمة من الأشخاص المصدر لهم شهادات تصديق، ويعتبر هذا الالتزام أكثر الالتزامات دقة بالنسبة لعمل مؤدي الخدمات؛ إذ أنه يهدف إلى الربط التام بين معطيات وضع التوقيع ومعطيات التحقق من سلامته، ونسبته إلى الموقع[1]. ويتم التحقق من البيانات والمعلومات المقدمة بالاعتماد على كافة الوسائل القانونية الممكنة لضمان صحة هذه البيانات واتصالها بالشخص المعني، كاستعمال الأوراق الثبوتية من جواز سفر أو بطاقة التعريف الوطنية والمهنية وغيرها من الوثائق[2].

نص المشرع الجزائري على هذا الالتزام من خلال المادة (44 ف1) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين والتي جاء نصها كالآتي: «**يجب على مؤدي خدمات التصديق الإلكتروني، قبل منح شهادة التصديق الإلكتروني، أن يتحقق من تكامل بيانات الإنشاء مع بيانات التحقق من التوقيع...**». كما نص عليها المشرع التونسي بموجب الفصل (18) من القانون (83 لسنة 2000) المتعلق بالمبادلات والتجارة الإلكترونية على أن: «**يضمن مزود خدمات المصادقة الإلكترونية:**

-صحة المعلومات المصادق عليها التي تضمنتها الشهادة في تاريخ تسليمها...»، أما عن المشرع المغربي فقد نص هو الآخر على هذا الالتزام في المادة (21) من القانون (05-53) المتعلق بالتبادل الإلكتروني للمعطيات القانونية، إذ نص بموجب الفقرة الأخيرة من هذه المادة على أنه: «**... 2- بالتأكد وقت تسليم الشهادة الإلكترونية من أن:**

أ- المعلومات التي تحتوي عليها صحيحة،

ب- الموقع المشار فيها إلى هويته يمتلك معطيات لإنشاء التوقيع الإلكتروني تطابق معطيات التحقق من التوقيع الإلكتروني المضمنة في الشهادة».

---

(1)- Didier GOBERT, Cadre juridique pour la signatures éléctroniques et les services de certification: analyse de la loi du 9 juillet 2001. Formation permanant CUP, volume 54, mars 2002, p 19.
Cadre juridique pour les signatures électroniques... Catalogue en ligne (docs-crids.eu)

(2)- زهيرة كيسي، مرجع سابق، ص 214.

ونظرا لأهمية هذه البيانات الشخصية، ألزمت التشريعات المتعلقة بالمعاملات الإلكترونية جهات التصديق الإلكتروني ببذل العناية اللازمة والمعقولة أثناء قيامها باستقبال هذه البيانات لصاحب طلب إصدار شهادة التصديق الإلكتروني[1]، لذا يُعد التزام مؤدي خدمات التصديق الإلكتروني في التأكد من صحة البيانات التزاما ببذل عناية، إذ تنص المادة (9/ب) من قانون اليونسترال النموذجي لسنة (2001) المتعلق بالتوقيعات الإلكترونية على: «... **أن يولي قدرا معقولا من العناية لضمان دقة واكتمال كل ما يقدمه من تأكيدات جوهرية ذات صلة بالشهادة طيلة دورة سريانها، أو مدرجة في الشهادة...**»، وكذا ما تنص عليه المادة (53 ف3) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين، والتي جاء نصها كالآتي: «**يكون مؤدي خدمات التصديق الإلكتروني الذي سلم شهادة تصديق إلكتروني موصوفة، مسؤولا عن الضرر الذي يلحق بأي هيئة أو شخص طبيعي أو معنوي، اعتمد على شهادة التصديق الإلكتروني هذه، وذلك فيما يخص: ...**

3 - التأكد من إمكانية استعمال بيانات إنشاء التوقيع، والتحقق منه بصفة متكاملة.

إلا في حالة ما إذا قدم مؤدي خدمات التصديق الإلكتروني ما يثبت أنه لم يرتكب أي إهمال».

ويتفرع عن الالتزام المتعلق بالتحقّق من صحة البيانات التزامات أخرى عديدة نشير إليها فيما يلي:

- لا يمكن لمؤدي خدمات التصديق الإلكتروني جمع البيانات الشخصية للموقع، إلا بعد موافقته الصريحة نظرا لأهمية وخطورة هذه المعلومات، وفي هذا الصدد نص المشرع الجزائري بموجب المادة (43 ف1) من القانون (15- 04) المتعلق بالتوقيع والتصديق الإلكترونيين الجزائري على أنه: «**لا يمكن مؤدي خدمات التصديق الإلكتروني جمع البيانات الشخصية للمعني، إلا بعد موافقته الصريحة...**». كما نص كذلك من خلال المادة (7ف1) من القانون (18-07) المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع

---

(1)- دحماني سمير، مرجع سابق، ص 119؛ **درار نسيمة**، التوثيق الرقمي ومسؤولية سلطات المصادقة الإلكترونية في القانون 15-04، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 09، المجلد02، مارس 2018، ص 860.

الشخصي[1]، بأنه: **«لا يمكن القيام بمعالجة المعطيات ذات الطابع الشخصي إلا بالموافقة الصريحة للشخص المعني...».**

كما نص المشرع التونسي بموجب الفصل (1/16) من القانون (83 لسنة 2000) المتعلق بالمبادلات والتجارة الإلكترونية على أنه: **«يتولى مزود خدمات المصادقة الإلكترونية، عند طلب شهادة جمع المعلومات ذات الصبغة الشخصية مباشرة من الشخص المعني وله أن يتحصل عليها من الغير بعد الموافقة الكتابية أو الإلكترونية لهذا الشخص...»**، كما ألزم المشرع الفرنسي هو الآخر بموجب المادة (7) من القانون رقم (2004-801) المؤرخ في (06 أوت 2004) المتعلق بحماية الأشخاص الطبيعية لدى معالجة المعطيات ذات الطابع الشخصي، المعدل للقانون (78-17) المؤرخ في (06 جانفي 1978) المتعلق بالإعلام الآلي والحريات[2]، المسؤول عن آلية معالجة المعطيات الشخصية بوجوب الحصول على الموافقة الصريحة للشخص المعني قبل الحصول على معطياته الشخصية.

- يجب على مؤدي خدمات التصديق جمع المعلومات الشخصية الضرورية فقط لمنح وحفظ شهادة التصديق الإلكتروني، ولا يمكن له أن يستعملها لأغراض أخرى خارج إطار نشاط التصديق الإلكتروني، ولذلك نص المشرع الجزائري بموجب المادة (43 ف 2) من القانون (15- 04) المتعلق بالتوقيع والتصديق الإلكترونيين سالف الذكر على أنه: **«... ولا يمكن مؤدي خدمات التصديق الإلكتروني، أن يجمع إلا البيانات الشخصية الضرورية لمنح وحفظ**

---

(1)- قانون رقم (18-07) مؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج.ر.ع 34.

(2)- Loi n° 2004-801 du 6 aout 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. J.O.R.F, n° 182 du 07 aout 2004.
http://www.legifrence.fr

- Art 07 du la loi 2004-801 **: « Un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée ou satisfaire à l'une des conditions suivantes :**
1° Le respect d'une obligation légale incombant au responsable du traitement ;
2° La sauvegarde de la vie de la personne concernée ;
3° L'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement ;
4° L'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci ;
5° La réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée ».

شهادة التصديق الإلكتروني، ولا يمكن استعمال هذه البيانات لأغراض أخرى»، وأكد المشرع التونسي على هذا الالتزام من خلال الفصل (2/16 و3) من القانون (83 لسنة 2000) المتعلق بالمبادلات والتجارة الإلكترونية على أنه: «... **يحجر على مزود خدمات المصادقة الإلكترونية جمع المعلومات التي لا تكون ضرورية لتسليم الشهادة.**

ويحجر عليه استعمال المعلومات التي جمعها بغرض تسليم الشهادة خارج إطار أنشطة المصادقة، ما لم يتحصل كتابيا أو إلكترونيا على موافقة الشخص المعني»، ويحق لصاحب الشهادة سحب الموافقة في أي وقت [1].

ثانيا: الالتزام بالحفاظ على سرية البيانات

يقصد بهذا الالتزام الحفاظ على سرية البيانات ذات الطابع الشخصي المقدمة من العميل إلى الجهة المختصة بإصدار شهادة التصديق الإلكترونية، بهدف حفظها أو تبادلها أو استخدامها في إنشاء مفاتيح التصديق الإلكتروني وإصدار شهـــادة المصادقة الإلكترونيـــة [2]، ويترتب على ذلك أنه لا يجوز استعمال هذه المعلومات إلا للضرورة القصوى وبهدف استخراج شهادة المصادقة الإلكترونية [3].

يعتبر هذا الالتزام من الالتزامات المهمة الملقاة على عاتق مؤدي خدمات التصديق الإلكتروني، نظرا لخصوصية هذه البيانات الراجعة لطابعها الشخصي، فلا يجوز نشرها إلا وفقا لما يسمح به القانون.

---

(1)- ينص المشرع التونسي بموجب الفصل 38 من القانون 83 لسنة 2000 المتعلق بالمبادلات والتجارة الإلكترونية على أنه: «**لا يمكن لمزود خدمات المصادقة الإلكترونية معالجة المعطيات الشخصية إلا بعد موافقة صاحب الشهادة المعني.**

ويمكن اعتماد الإعلام الإلكتروني بالموافقة إذا ضمن المزود:

- **إعلام صاحب الشهادة بحقه في سحب الموافقة في كل وقت،**
- **إمكانية تحديد هوية الأطراف المستعملة للمعطيات الشخصية،**
- **الاحتفاظ بحجة الموافقة التي لا يمكن تغييرها»**

(2)- **عيسى غسان ربضي**، مرجع سابق، ص 151.

(3)- Didier GOBERT, Cadre juridique pour la signatures éléctroniques et les services de certification, op.cit, p 18.

ولقد نص المشرع الجزائري على وجوب الحفاظ على سرية البيانات الشخصية للموقع من خلال المادة (42) من القانون (15-04) سالف الذكر، إذ تنص هذه المادة على أنه: «**يجب على مؤدي خدمات التصديق الإلكتروني الحفاظ على سرية البيانات والمعلومات المتعلقة بشهادات التصديق الإلكتروني الممنوحة**». في حين أكّد المشرع التونسي على ضرورة احترام هذا الالتزام من خلال الفصل (15) من القانون (83 لسنة 2000) المتعلق بالمبادلات والتجارة الإلكترونية، سالف الذكر، حيث تنص هذه المادة على أنه: «**يتعين على مزودي خدمات المصادقة الإلكترونية وأعوانهم المحافظة على سرية المعلومات التي عهدت إليهم في إطار تعاطي أنشطتهم باستثناء تلك التي رخص صاحب الشهادة كتابيا أو إلكترونيا في نشرها أو الإعلام بها أو في الحالات المنصوص عليها في التشريع الجاري به العمل**».

أما بالنسبة للمشرع المصري فقد نص على ضرورة الحفاظ على سرية هذه البيانات بموجب المادة (21) من القانون (15 لسنة 2004) المتعلق بالتوقيع الإلكتروني، وذلك بالنص على أن: «**بيانات التوقيع الإلكتروني والوسائط الإلكترونية والمعلومات التي تقدم إلى الجهة المرخصة لها بإصدار شهادات التصديق الإلكتروني سرية، ولا يجوز لمن قدمت إليه أو اتصل بها بحكم عمله إفشاؤها للغير أو استخدامها في غير الغرض الذي قدمت من أجـــله**». ولم يكتف المشرع المصري بهذه المادة، بل نص على هذا الالتزام كذلك من خلال لائحته التنفيذية لقانون التوقيع الإلكتروني، وذلك من خلال المادة (12/ ح) على وجوب أن يتوافر لدى طالب الحصول على الترخيص بإصدار شهادات التصديق الإلكتروني المتطلبات التالية: «...- **نظام للحفظ على السرية الكاملة للأعمال المتعلقة بالخدمـات التـــي يرخـــص بها، وللبيانات الخاصة بالعملاء**،...».

كذلك الحال بالنسبة للمشرع المغربي إذ وضع على عاتق جهات المصادقة الإلكترونية الالتزام بالسرية خصوصا فيما يتعلق بالمعطيات ذات الطابع الشخصي المقدمة من طرف

العميل، بهدف حفظها أو تبادلها أو استخدامها في تأليف مفاتيح التوقيع الإلكتروني وإصدار شهادة إلكترونية معتمدة في هذا الخصوص [1].

وقد نص المشرع المغربي بموجب المادة (24) من القانون (05-53) المتعلق بالتبادل الإلكتروني للمعطيات القانونية على أن: «**يلزم مقدمو خدمات المصادقة الإلكترونية ومستخدموهم كذلك بكتمان السر المهني، تحت طائلة العقوبات المنصوص عليها في التشريع الجاري به العمل.**

يتحملون وفق القواعد القانونية العادية، مسؤولية تهاونهم أو قلة كفاءتهم أو قصورهم المهني سواء تجاه المتعاقدين أو تجاه الأغيار.

يجب على مقدمي خدمات المصادقة الإلكترونية أن يحافظوا على معطيات إنشاء الشهادة ويلزمـــون، بأمر من وكيل الملك، بتبليغها إلى السلطات القضائية، وذلك وفق الشروط المنصوص عليها في التشريع الجاري به العمل.

وفي هذه الحالة، وعلى الرغم من كل المقتضيات التشريعية المخالفة يتولى مقدمو خدمات المصادقة الإلكترونية إخبار المستعملين المعنيين على الفور.

لا تطبق إلزامية كتمان السر المهني، المشار إليها في الفقرة الأولى أعلاه:

- **تجاه أعوان السلطة الوطنية وخبرائها والأعوان والضباط المشار إليهم في المادة 41 أدناه خلال ممارسة الصلاحيات المنصوص عليها في المادتين 19 و41 من هذا القانون؛**
- **إذا وافق صاحب التوقيع الإلكتروني على نشر أو تبليغ المعلومات المدلى بها إلى مقدم خدمات المصادقة الإلكترونية».**

نلاحظ من خلال ما سبق ذكره، إلزام تشريعات الإثبات الإلكتروني جهات التصديق الإلكتروني بضمان سلامة وسرية المعطيات الشخصية للموقع؛ نظرا لطابعها الشخصي وحرمة الحياة الخاصة التي تتطلب السرية والحيطة في معالجتها.

---

(1)- عبد الحكيم زروق، مرجع سابق، ص 52.

الفرع الثاني
الالتزامات المتعلقة بشهادة التصديق الإلكترونية

يعتبر إصدار شهادة التصديق الإلكتروني من أهم الالتزامات التي تقع على عاتق جهات التصديق الإلكتروني؛ لما لها من أهمية كبيرة في إثبات هوية صاحب التوقيع الإلكتروني ونسبته له، واستفائه للشروط والضوابط المطلوبة فيه. إلى جانب ذلك تقوم شهادة التصديق الإلكتروني على ضمان سلامة التوقيع الإلكتروني وبالتالي المحرر الإلكتروني الذي يتضمنـــــه إذ تؤكد الشهادة صحة البيانات المُوَّقَع عليها وأنها صادرة من المُوقِع ولم يتم التلاعب بها أو تعديلها.

ولأهمية الدور الذي تقوم به شهادة التصديق الإلكترونية تطرقت تشريعات الإثبات الإلكتروني إلى نظام إصدارها **(أولا)**، وكذا إلغائها **(ثانيا)**، وحتى مسألة الاعتراف القانوني بالشهادات الأجنبية **(ثالثا)**.

أولا: الالتزام بإصدار شهادة التصديق الإلكتروني

ألزمت تشريعات الإثبات الإلكتروني جهات التصديق الإلكتروني بإصدار شهادات تصديق إلكترونية، تؤكد هوية صاحب التوقيع الإلكتروني وارتباطه بالمحرر الإلكتروني، وهذا ما أشارت إليه معظم التشريعات المتعلقة بالمعاملات الإلكترونية، فقد نص قانون اليونسترال النموذجي لسنة (2001) بشأن التوقيعات الإلكترونية، بموجب المادة (2/هـ) على أن: «**مقدم خدمات التصديق يعني شخصا يصدر الشهادات ويجوز ان يقدم خدمات أخرى ذات صلة بالتوقيعات الإلكترونية**»، وقد نصت العديد من التشريعات الوطنية[1] على هذا الالتزام، فما المقصود بشهادة التصديق الإلكتروني؟

1-تعريف شهادة التصديق الإلكتروني:

(1)- أنظر في هذا الصدد: المادة 41 من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين الجزائري؛ الفصل 12 من قانون المبادلات والتجارة الإلكترونية 85 لسنة 2000 التونسي؛ المادة 46 من الترخيص رقم 2006/103 الصادر عن هيئة تنمية صناعة التكنولوجيا لجمهورية مصر العربية، يتضمن منح ترخيص بتقديم خدمات التوقيع الإلكتروني.

تعددت التعريفات الموضحة لشهادة التصديق الإلكتروني، مثلما تعددت مسمياتها[1]، لتعدد التشريعات المنظمة للمعاملات الإلكترونية، فعرفها قانون اليونسترال النموذجي لسنة (2001) المتعلق بالتوقيعات الإلكترونية بموجب المادة (2/ب) منه على أنها: **«"شهادة" تعني رسالة بيانات أو سجلا آخر يؤكدان الارتباط بين الموقع وبيانات إنشاء التوقيع»**، لقد ذكر هذا التعريف طبيعة الشهادة بأنها عبارة عن رسالة بيانات، كما بيّن الغاية من إصدارها وهي إثبات الصلة بين الموقع وبيانات إنشاء التوقيع، إلا أنه لم يحدد من خلال هذا التعريف الجهة المصدرة لهذه الشهادة، ومما يعاب على هذا التعريف أنه ربط بين الموقع وبيانات إنشاء التوقيع؛ أي المفتاح الخاص؛ بينما ما يلزم لتأكيد ارتباط التوقيع بالموقع هي بيانات التحقق من التوقيع، أو ما يقصد بالمفتاح العام والذي يمكن الإفصاح عنه للغير.

كما أورد التنظيم الأوروبي (910-2014) تعريفا لها من خلال المادة (14/3)[2] بأنها: **«شهادة إلكترونية ترتبط ببيانات التحقق من التوقيع الإلكتروني لشخص طبيعي وتؤكد على الأقل اسمه الحقيقي أو اسمه المستعار»**. بيّن التنظيم الأوروبي من خلال هذا التعريف طبيعة شهادة التصديق، كما أنه لم يقع في الخطأ الذي وقع فيه قانون اليونسترال، حيث ربط الموقع ببيانات التحقق، أي المفتاح العام.

أما عن التشريعات العربية، فنجد أن المشرع المصري عّرف شهادة التصديق في المادة (1/و) من قانون التوقيع الكتروني المصري (15 لسنة 2004) بأنها: **«شهادة التصديق الإلكتروني: الشهادة التي تصدر من الجهة المرخص لها بالتصديق وتثبت الارتباط بين الموقع وبيانات إنشاء التوقيع»**، وهو التعريف ذاته الذي تضمنته المادة (8/1) من اللائحة التنفيذية. إن هذا التعريف يشبه إلى حد كبير التعريف الذي جاء به قانون اليونسترال لسنة (2001) المتعلق بالتوقيعات الإلكترونية، حيث أنه لم يبيّن الجهة المصدرة للشهادة ولا

---

(1)- أطلقت عليها عدة تسميات منها: "**الشهادة**"، "**شهادة التوثيق**"، "**شهادة التوثيق الإلكتروني**"، "**شهادة المصادقة الإلكتروني**"، " **شهادة التصديق الإلكترونية**" وهي التسمية التي اعتمدها المشرع الجزائري بموجب القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين.

(2)- Article 3/14 du règlement n° 910-2014 : «**… «certificat de signature électronique», une attestation électronique qui associe les données de validation d'une signature électronique à une personne physique et confirme au moins le nom ou le pseudonyme de cette personne;… ».**

طبيعتها، إضافة إلى ذلك وقع في نفس العيب الذي وقع فيه قانون اليونسترال؛ حيث ربط بين الموقع ومفتاحه الخاص بدل العام.

في حين أن المشرع التونسي قد عرّف شهادة التصديق أو كما أطلق عليها " شهادة المصادقة الإلكترونية" بموجب الفصل (2) من القانون (83 لسنة 2000)، سالف الذكر بأنها: «- **شهادة المصادقة الإلكترونية: الوثيقة الإلكترونية المؤمنة بواسطة الإمضاء الإلكتروني للشخص الذي أصدرها والذي يشهد من خلالها، إثر المعاينة، على صحة البيانات التي تتضمنها**»، ما يعني أن المشرع التونسي قد بيّن طبيعة الشهادة بوصفها وثيقة إلكترونية، وحدد وظيفتها المتمثلة في إثبات صحة البيانات التي تتضمنها، غير أنه لم يتطرق إلى الجهة المصدرة لها.

نص المشرع الأردني في المادة (2) من قانون المعاملات الإلكترونية (15 لسنة 2015) على أن: «**"شهادة التوثيق الإلكتروني" الشهادة الصادرة عن جهة التوثيق الإلكتروني لإثبات نسبة توقيع إلكتروني إلى شخص معين استنادا إلى إجراءات توثيق معتمدة**». نلاحظ من خلال هذه المادة أن المشرع الأردني قد حدد الهدف من وراء إصدار هذه الشهادة وهي إثبات نسبة التوقيع إلى الموقع، كما بين الجهة المصدرة للشهادة.

بينما عرفها المشرع المغربي بطريقة عكسية بموجب المادة (10) من القانون (05-53) المتعلق بالتبادل الإلكتروني للمعطيات القانونية، والتي جاء نصها كالآتي: «**تُثبَت العلاقة بين المعطيات التي تمكن من التحقق من التوقيع الإلكتروني والموقع بشهادة إلكترونية. وتتمثل هذه الشهادة في سند يتم إعداده بشكل إلكتروني.**

يمكن أن تكون الشهادة الإلكترونية المذكورة بسيطة أو مؤمنة»، بيّن المشرع المغربي طبيعة الشهادة؛ إذ نص على أن تكون في شكل إلكتروني، كما نص على الهدف منها وهي الربط بين بيانات التحقق من التوقيع -المفتاح العام-، وبين المُوقِع، إضافة إلى ذلك قسم الشهادة إلى نوعين شهادة إلكترونية بسيطة وشهادة إلكترونية مؤمنة.

وقد تطرق من خلال المادة (11) من القانون نفسه للشهادة الإلكترونية المؤمنة، وقد بين أنها تصدر عن مقدم لخدمات المصادقة الإلكترونية معتمد، وأن تتضمن معطيات محددة نصت عليها المادة نفسها.

بالرجوع للمشرع الجزائري، نجده قد ميّز بين نوعين من شهادات التصديق الإلكتروني (البسيطة والموصوفة)، إذ عرّف شهادة التصديق الإلكتروني البسيطة أو العادية بموجب المادة (7/2) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين، على أنها: **«وثيقة في شكل إلكتروني تثبت الصلة بين بيانات التحقق من التوقيع الإلكتروني والمـــوقع»**، من خلال هذا التعريف بين المشرع الجزائري طبيعة الشهادة؛ إذ اعتبرها وثيقة في شكل إلكتروني، كما أوضح الغاية منها وهي الربط بين الموقع ومفتاحه التشفيري العام، إلا أنه لم يحدد الجهة المصدرة للشهادة ولا البيانات الواردة فيها.

أما النوع الثاني فيتمثل في شهادة التصديق الإلكتروني الموصوفة، غير أنه لم يورد لها تعريفا من خلال المادة (2) من القانون (15-04) سالف الذكر، الخاصة بالتعاريف، ولكنه نظّم أحكامها ضمن المادة (15) من القانون نفسه، واعتبر أنها شهادة تصديق إلكتروني موصوفة تصدر عن مؤدي خدمات التصديق الإلكتروني، أو الطرف الثالث الموثوق، ذلك وفقا لسياسة التصديق الإلكتروني، وتمنح للمُوقِّع دون سواه، إضافة إلى تضمنها مجموعة من البيانات محددة بنص الفقرة الثالثة من المادة نفسها.

نستخلص من التعاريف السابقة، أن شهادة التصديق الإلكتروني عبارة عن وثيقة في شكل إلكتروني، تصدر عن جهات التصديق الإلكتروني وفقا لسياسة التصديق المعتمدة، تتضمن مجموعة من البيانات، هدفها الأساسي إثبات هوية الموقع والتأكد من صحة توقيعه، وكذا من البيانات التي تتضمنها المعاملة الإلكترونية.

2-البيانات الواجب توفرها في شهادة التصديق الإلكتروني:

تختلف شهادة التصديق الإلكتروني البسيطة عن المؤمنة في كونها لا تتضمن على جميع البيانات التي أوجبها القانون، على عكس شهادة التصديق الإلكتروني المؤمنة أو الموصوفة، إذ تحوي كل البيانات الجوهرية المحددة قانونا والتي تشكل مقتضيات أمان المتعاملين.

وقد أوردت العديد من تشريعات الإثبات الإلكتروني هذه البيانات ضمن نصوصها القانونية[1]، وكذلك الأمر بالنسبة للمشرع الجزائري الذي نص عليها من خلال المادة (15) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين، والتي جاء نصها كالآتي: «**شهادة التصديق الإلكتروني الموصوفة هي شهادة تصديق إلكتروني تتوفر فيها المتطلبات الآتية:**

1- أن تمنح من قبل طرف ثالث موثوق أو من قبل مؤدي خدمات تصديق إلكتروني، طبقا لسياسة التصديق الإلكتروني[2] الموافق عليها،

2- أن تمنح للموقع دون سواه،

3- يجب أن تتضمن على الخصوص،

أ- إشارة تدل على أنه تم منح هذه الشهادة على أساس أنها شهادة تصديق إلكتروني موصوفة،

ب- تحديد هوية الطرف الثالث الموثوق أو مؤدي خدمات التصديق الإلكتروني المرخص له المصدر لشهادة التصديق الإلكتروني وكذا البلد الذي يقيم فيه،

ج- اسم الموقع أو الاسم المستعار الذي يسمح بتحديد هويته،

د- إمكانية إدراج صفة خاصة للموقع عند الاقتضاء، وذلك حسب الغرض من استعمال شهادة التصديق الإلكتروني،

---

(1)- على الرغم من اختلاف صياغة هذه البيانات من قانون لآخر إلى أنها تصب في نفس المعنى، وللاطلاع أكثر على هذه البيانات راجع كل من: الملحق (1) من التنظيم الأوروبي رقم (910-2014)؛ المادة (11) من القانون (05-53) المتعلق بالتبادل الإلكتروني للمعطيات القانونية المغربي؛ المادة (20) من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري؛ الفصل (17) من الباب الرابع من قانون المبادلات والتجارة الإلكترونية التونسي (83 لسنة 2000).

(2)- تنص المادة (2 ف15) من القانون (15-04) على أن: «**سياسة التصديق الإلكتروني: مجموع القواعد والإجراءات التنظيمية والتقنية المتعلقة بالتوقيع والتصديق الإلكتروني** ».

هـ- بيانات تتعلق بالتحقق من التوقيع الإلكتروني، وتكون موافقة لبيانات إنشاء التوقيع الإلكتروني،

و- الإشارة إلى بداية ونهاية مدة صلاحية شهادة التصديق الإلكتروني،

ز- رمز تعريف شهادة التصديق الإلكتروني،

- التوقيع الإلكتروني الموصوف لمؤدي خدمات التصديق الإلكتروني أو للطرف الثالث الموثوق الذي يمنح شهادة التصديق الإلكتروني،

ط- حدود استعمال شهادة التصديق الإلكتروني، عند الاقتضاء،

ي- حدود قيمة المعاملات التي قد تستعمل من أجلها شهـادة التصديق الإلكتروني، عند الاقتضاء.

ك- الإشارة إلى الوثيقة التي تثبت تمثيل شخص طبيعي أو معنوي أخر، عند الاقتضاء».

وعليه، لكي تكتسب شهادة التصديق الإلكتروني صفة الشهادة الموصوفة -المؤمنة- وجب احتوائها على البيانات التالية:

- الإشارة إلى ما يفيد أن هذه الشهادة هي شهادة تصديق إلكتروني موصوفة: والغرض من ذلك هو إتاحة الفرصة للمستخدم لتقدير درجة الأمان التي تتمتع بها شهادة التصديق الإلكتروني الموصوفة، باعتبار أن لهذه الشهادة كامل الحجية في الإثبات، وذلك راجع للمستوى الذي تم منحه لهذه الشهادة بصفتها موصوفة.

-**هوية مزود خدمات التصديق:** وذلك بذكر اسمه وعنوانه ومقره الرئيسي وكيانه القانونـي، والدولة التي نشأ بـها لممارسة اختصـاصه، وهذا يزيد من الثقـة لدى المتعـاملين، وكذلك يمكن من الرجوع على مزود الخدمة في حال قيام مسؤوليته.

-**هوية صاحب الشهادة:** وهو من صدرت الشهادة باسمه وبناء على طلبه، ويجب أن تشمل الشهادة على ما يحدد شخصية الموقع، وذلك من خلال بيان اسم الموقع الفعلي أو اسمه المستعار الذي يسمح بتحديد هويته، وفي حال استخدام الاسم المستعار لصاحب التوقيع وجب

على مؤدي خدمات التصديق الإلكتروني حفظ الهوية الحقيقية المرتبطة بالاسم المستعار، وذلك لأجل استعمالها في حال وجود رقابة من طرف السلطات المختصة [1].

- **صفة صاحب التوقيع:** نلاحظ أن المشرع الجزائري لم يجعل هذا الشرط ضروريا وذلك بذكره مصطلح (عند الاقتضاء)، والحكمة من هذا البيان راجعة إلى تنوع صفة طالب الشهـــادة، فقد يتم طلب الشهادة بصفة شخصية، كما قد يتم طلبها من قبل العاملين بالقطاع الحكومي أو القطاع الخاص[2].

-**بيانات التحقق من صحة التوقيع الإلكتروني:** ويقصد بها هنا مفتاح التشفير العام المقابل لمفتاح التشفير الخاص، الذي يؤكد أن الرسالة صادرة من المرسل نفسه ولم تتعرض لأي تزير أو تحريف.

-**مدة صلاحية الشهادة:** هذا البيان مهم للأطراف المتعاقدة، وذلك لأنه يحقق الثقة عند تعاملهم مع صاحب الشهادة، لأن الشهادات عادة تصدر لفترة محدودة وبمجرد انتهاء تاريخ صلاحيتها تصبح غير قابلة للاستعمال، ويتم رفضها تلقائيا من قبل برمجيات مستقبل الرسالة الإلكترونية[3]، والهدف من هذا البيان هو إمكانية تأكد الشخص من أن التوقيع الإلكتروني قد تم إنشاءه خلال الفترة التشغيلية أو المدة الزمنية المحددة، وبالرغم من إدراج المشرع الجزائري لهذا البيان، وأهميته البالغة، إلا أنه وبالمقابل لم يحدد المدة الزمنية لصلاحية الشهادة.

- **الرقم التسلسلي للشهادة:** أي منح الشهادة رقما معينا، وذلك وفق قاعدة بيانات متوافرة لدى جهة التوثيق.

---

(1)- الزهرة بره، جميلة حميدة، شهادة التصديق الإلكتروني كآلية لتعزيز الثقة في المعاملات الإلكترونية، مجلة العلوم القانونية والسياسية، المجلد 10، العدد1، أفريل 2019، ص 896.

(2)- عبير مخائيل الصفدي، النظام القانوني لجهات توثيق التوقيع الإلكتروني، رسالة ماجستير في القانون الخاص، جامعة الشرق الأوسط، الأردن، 2009، ص 93.

(3)- عبير مخائيل الصفدي، المرجع نفسه، ص 93.

- **التوقيع الإلكتروني لجهة التصديق:** يجب احتواء شهادة التصديق على التوقيع الإلكتروني الموصوف لمقدم خدمات التصديق الإلكتروني، وذلك لتأكيد صحة محتويات الشهادة وسلامة المعلومات الواردة بها

-**تحديد قيمة ونوع المعاملات التي تستخدم بشأنها الشهادة:** يشير المشرع الجزائري إلى أنه يجوز عند الاقتضاء أن تتضمن شهادة التصديق نوع المعاملات المسموح بها، وكذلك الحد الأقصى لقيمة هذه المعاملات، فإذا فاق استخدامها الحد المعين بها انتفت المسؤولية عن جهة التصديق، ويعد إهمالا وتقصيرا من الشخص الذي اعتمد على هذه الشهادة.

-**الإشارة إلى الوثيقة التي تثبت تمثيل شخص طبيعي أو معنوي آخر:** في حال كان صاحب الشهادة ممثلا لشخص آخر -شخص طبيعي أو معنوي-، وجب الإشارة إلى ذلك ضمن شهادة التصديق مع بيان الوثائق التي تثبت واقعة التمثيل.

نلاحظ من خلال هذه البيانات، أنها تتضمن جميع المعلومات الأساسية الخاصة بمقدم خدمات التصديق، وكذا المعلومات والبيانات المتعلقة بصاحب التوقيع، وكل المعلومات التي وجب أن تشملها الشهادة. ويكمن الهدف من وراء إلزام جهات التصديق الإلكتروني من ذكر كل هذه البيانات المنصوص عليها في شهادة التصديق الإلكتروني، هو منحها الحجية القانونية الكاملة والتعويل عليها في مجال الإثبات.

ثانيا: الالتزام بتعليق أو إلغاء شهادة التصديق الإلكتروني:

يلتزم مؤدي خدمات التصديق الإلكتروني بتعليق العمل بشهادة التصديق الإلكتروني أو إلغائها في حال وجود سبب يوجب ذلك، ويجب عدم التراخي في اتخاذ هذا الإجراء لتجنب العواقب الوخيمة التي قد تنجر عن عدم وقف العمل بالشهادة إما مؤقتا أو بشكل نهائي؛ كعقد صفقات، أو إجراء تحويلا نقدية، أو إصدار أوامر شراء، أو بيع بشهادات إلكترونية مشكوك فيها أو غير صحيحة.

نصت العديد من تشريعات الإثبات الإلكتروني على حالات وجوب تعليق أو إلغاء شهادات التصديق الإلكتروني[1]، أما عن المشرع الجزائري فقد بين حالات إلغاء العمل بشهادة التصديق الإلكتروني وفقا لنص المادة (45) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين، إلا أنه لم يتطرق لحالات تعليق العمل بهذه الشهادة، ولربما يعود ذلك إلى اعتباره أن حالات الإيقاف المؤقت للشهادة من الإجراءات البديهية التي تسبق الفصل في إلغائها. غير أننا نرى أن عدم تنظيم المشرع الجزائري لمسألة تعليق العمل بشهادة التصديق الإلكتروني واكتفائه بالنص على حالات إلغائها يُعد تقصيرا من جانبه؛ لكونه أمرا مهما قد ينجر عن عدم تنظيمه عواقب وخيمة قد تضر بالأشخاص المعتمدين على هذه الشهادة.

1- حالات تعليق العمل بشهادة التصديق الإلكتروني:

يقصد بتعليق العمل بشهادة التصديق الإلكتروني الوقف المؤقت لسريان الشهادة؛ أي تعطيل العمل بالأثر القانوني المترتب عليها تمهيدا لإلغائها أو استئناف العمل بها متى ثبت عدم صحة السبب الذي أدى إلى تعليقها [2].

وبما أننا أشرنا سابقا إلى أن المشرع الجزائري لم ينص على حالات تعليق العمل بشهادة التصديق الإلكتروني، فسنتطرق إلى هذه الحالات من خلال قانون المبادلات والتجارة التونسي (83 لسنة 2000)، والذي نص على أنه يتولى مزود خدمات المصادقة الإلكترونية تعليق العمل بشهادة المصادقة حالا بطلب من صاحبها أو عندما يتبين:

-أن الشهادة سلمت بالاعتماد على معلومات مغلوطة أو مزيفة.

---

(1)- نصت العديد من تشريعات الإثبات الإلكتروني على حالات تعليق وإلغاء العمل بشهادة التصديق الإلكتروني ومنها: المشرع التونسي بموجب الفصلين (19 و20) من قانون المبادلات والتجارة الإلكتروني (83 لسنة 2000) ويعتبر القانون الذي فصل بشكل دقيق حالات تعليق العمل بشهادة التصديق الإلكتروني؛ في حين نص المشرع المصري على حالات الإلغاء الكلي للشهادة وفقا للمادة (12 /ط) من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري؛ ونجد أن المشرع المغربي هو الآخر لم ينص على حالات الإيقاف المؤقت للشهادة مثلما فعل المشرع التونسي وإنما نص على حالات الإلغاء الكلي وفقا للفصل (21ف3) من القانون (05-53) المتعلق بالتبادل الإلكتروني للمعطيات القانونية.

(2)- **الزهرة بره، جميلة حميدة**، مرجع سابق، ص 903؛ **عبد الفتا بيومي حجازي**، التوقيع الإلكتروني في النظم القانونية المقارنة، مرجع سابق، ص 173.

- أنه تم انتهاك منظومة إحداث الإمضاء.
- أن الشهادة استعملت بغرض التدليس.
- أن المعلومات المتضمنة بالشهادة قد تغيرت.

ويتولى مزود خدمات المصادقة الإلكترونية إعلام صاحب الشهادة حالا بالتعليق وسببـــه، ويتم رفع هذا التعليق حالا إذا تبينت صحة المعلومات المدونة بالشهادة وباستعمالها بصفة شرعية، ويعارض صاحب الشهادة أو الغير بقرار مزود الخدمات الخاص بتعليق الشهادة من تاريخ نشره بالسجل الإلكتروني [1].

2-حالات إلغاء العمل بشهادة التصديق الإلكتروني:

الإلغاء يعني الوقف الكلي للعمل بشهادة التصديق الإلكتروني وانعدام الأثر القانوني المترتب عليها بمجرد توافر الحالات المنصوص عليها قانونا، وقد حدد المشرع الجزائري حالات الإلغاء بموجب المادة (45)[2] من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكتروني، وتتمثل هذه الحالات في:

---

(1)- أنظر الفصل (19) من قانون المبادلات والتجارة التونسي (83 لسنة 2000).

(2)- تنص المادة (45) من القانون (15- 04) المتعلق بالتوقيع والتصديق الإلكترونيين، سالف الذكر، على أنه: «**يلغي مؤدي خدمات التصديق الإلكتروني شهادة التصديق الإلكتروني في الآجال المحددة في سياسة التصديق، بناء على طلب صاحب شهادة التصديق الإلكتروني الموصوفة الذي سبق تحديد هويته.**

ويلغي مؤدي خدمات التصديق الإلكتروني أيضا شهادة التصديق الإلكتروني الموصوفة عندما يتبين:

1- انه قد تم منحها بناء على معلومات خاطئة أو مزورة، أو إذا أصبحت المعلومات الواردة في شهادة التصديق الإلكتروني غير مطابقة للواقع، أو إذا تم انتهاك سرية بيانات إنشاء التوقيع،

2- أنها لم تصبح مطابقة لسياسة التصديق،

3- أنه تم إعلام مؤدي خدمات التصديق الإلكتروني بوفاة الشخص الطبيعي أو بحل الشخص المعنوي صاحب شهادة التصديق الإلكتروني.

يجب على مؤدي خدمات التصديق الإلكتروني إخطار صاحب شهادة التصديق الإلكتروني الموصوفة بإلغاء هذه الأخيرة مع تسبيب ذلك.

يجب على مؤدي خدمات التصديق الإلكتروني تبليغ صاحب شهادة التصديق الإلكتروني الموصوفة بانتهاء مدة صلاحيتها، في الآجال المحددة في سياسة التصديق. =

أ- إلغاء شهادة التصديق الإلكتروني بناء على طلب صاحبها:

بما أن شهادة التصديق الإلكتروني خاصة بصاحبها -سواء كان شخص طبيعي أو معنوي- وتصدر بناء على طلبـــه. وبالتالي هو الوحيد الذي يحق له طلب فإلغائها، وهو غير ملزم بذكر أي سبب أو مبرر في طلبه، وما على مؤدي خدمات التصديق الإلكتروني سوى التحقق من أن طالب الإلغاء هو صاحب الشهادة الفعلي[1].

تتعدد الأسباب التي قد تدفع صاحب الشهادة إلى طلب إلغائها، فقد يطلع الغير على منظومة تشغيل التوقيع الإلكتروني، أو يفقد مفتاحه الخاص، وغير ذلك من الأسباب، وطلب إلغاء الشهادة هو حق خاص بصاحبها فقط، وفي حال ما إذا تعلق بهذه الشهادة حق للغير، فإن هذا الغير لا يملك أن يطلب عدم إلغائها، وإنما يقتصر حقه في الرجوع على صاحب الشهادة بالتعويض إذا ما لحقه ضرر من استعمال الشهادة [2].

ب- أن تسلم الشهادة بناء على معلومات مغلوطة أو مزيفة:

إذا تبين لمؤدي خدمات التصديق الإلكتروني أنه سلم الشهادة بناء على معلومات مغلوطة؛ كما لو تضمنت بالخطأ اسم شخص آخر غير الذي طلب إصدارها، أو خطأ في تحديد قيمة المعاملات المسموح بها، أو أن يقوم بتسليم الشهادة أيضا بناء على معلومات مزورة؛ كأن يقوم صاحب التوقيع بتزوير بطاقته الشخصية أو جواز سفره ويقدمها لمؤدي خدمات التصديق الإلكتروني[3]، ففي كلتا الحالتين وجب على مؤدي خدمات التصديق الإلكتروني أن يقوم فورا بإلغاء العمل بشهادة التصديق الإلكتروني وإلا تحمل مسؤولية التأخر في اتخاذ الإجراءات اللازمة.

=يعتبر إلغاء شهادة التصديق الإلكتروني الموصوفة نهائيا».

(1)- صليحة مربا، دور التصديق الإلكتروني في إثبات المعاملات الإلكترونية وحفظها، مجلة الدراسات القانونية المقارنة، المجلد 07، العدد 01، 2021، ص 881.

(2)- علاء التميمي، الجهة المختصة بإصدار شهادة التصديق الإلكتروني، دار النهضة العربية، مصر، 2011، ص 57.

(3)- عبد الفتا بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، مرجع سابق، ص177.

ج-حالة تغير البيانات التي تتضمنها الشهادة:

من المفترض أن تبقى البيانات التي تحتويها الشهادة صحيحة طوال فترة سريانها، لكن قد يحدث وأن تتغير هذه البيانات؛ كأن يتعرض صاحب الشهادة إلى الإفلاس أو فقدان الأهلية أو تغيير الموطن أو الجنسيـــــة...الخ، مما يجعلها غير مطابقة للواقع، وعليه يلزم مؤدي خدمات التصديق بإلغاء العمل بهذه الشهادة.

د-حالة انتهاك سرية بيانات إنشاء التوقيع:

إذا ثبت انتهاك أو التلاعب بمنظومة إنشاء التوقيع الإلكتروني، وجب على مؤدي خدمات التصديق إلغاء العمل بهذه الشهادة فورا.

هـ-حالة عدم مطابقة الشهادة لسياسة التصديق:

المقصود بها أن شهادة التصديق الإلكتروني لم تعد تتلاءم مع القواعد والإجراءات التنظيمية والتقنية المتعلقة بالتوقيع والتصديق الإلكترونيين.

-حالة وفاة لشخص الطبيعي أو انحلال الشخص المعنوي صحاب الشهادة:

تعتبر شهادة التصديق الإلكتروني من الوثائق اللصيقة بصاحبها، وعليه فبمجرد وفاة الشخص الطبيعي أو انحلال الشخص المعنوي وجب إبلاغ مؤدي خدمات التصديق ليقوم بإلغاء العمل بالشهادة.

خ- حالة انتهاء مدة صلاحية الشهادة:

تعتبر مدة صلاحية الشهادة من بين البيانات الإلزامية التي فرضها المشـرع الجزائري، والتي يجب على مؤدي خدمات التصديق ذكرها والتأكد منها عند إصداره لشهادة التصديق، فتحديد مدة صلاحية الشهادة ضروري لصاحب الشهادة والغير، لمعرفة مدى صلاحية الاعتماد عليها، واشترط القانون تبليغ صاحب الشهادة قبل انتهاء فترة صلاحيتها من باب التنبيه والاحتياط حتى لا يقع في غلط مع الغيـــر، وفقا لنص المادة 45 من القانون (15-04).

أخيرا؛ يقع على مؤدي خدمات التصديق الإلكتروني التزامات أخرى بصدد إلغاء شهادة التصديق الإلكتروني وهي:

– إخطار صاحب شهادة التصديق الإلكتروني الموصوفة بإلغاء هذه الأخيرة مع تسبيب ذلك وفقا لنص المادة (45 ف 9) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين.

– يجب على مؤدي خدمات التصديق الإلكتروني، أخذ التدابير اللازمة من أجل الرد على طلب الإلغاء [1].

– يجب على مؤدي خدمات التصديق الإلكتروني تحويل المعلومات المتعلقة بشهادات التصديق الموصوفة بعد انتهاء صلاحيتها، إلى السلطة الاقتصادية للتصديق الإلكتروني من أجل حفظها [2].

– يحتج بالإلغاء اتجاه الغير ابتداء من تاريخ النشر، وفقا لسياسة التصديق الإلكتروني لمؤدي خدمات التصديق الإلكتروني [3].

نصل في الأخير، إلى أنه قد تعددت الالتزامات الملقاة على عاتق جهات التصديق الإلكتروني، بداية من شرط الحصول على الترخيص والتأهيل والذي يعتبر في الأصل أول التزام للقيام بنشاط التصديق، لتتنوع فيما بعد هذه الالتزامات، فيما بين تحقيق الأمن المعلوماتي

---

(1)– تنص المادة (46) من القانون (15– 04) المتعلق بالتوقيع والتصديق الإلكترونيين على أن: «**يتخذ مؤدي خدمات التصديق الإلكتروني، التدابير اللازمة من اجل الرد على طلب الإلغاء وفقا لسياسته للتصديق التي وافقت عليها السلطة الاقتصادية للتصديق الإلكتروني...**».

(2)– تنص المادة (47) من القانون (15– 04) المتعلق بالتوقيع والتصديق الإلكترونيين على أنه: «**يجب على مؤدي خدمات التصديق الإلكتروني تحويل المعلومات المتعلقة شهادات التصديق الإلكتروني الموصوفة بعد انتهاء صلاحيتها، إلى السلطة الاقتصادية للتصديق الإلكتروني من أجل حفظها**».

(3)– تنص المادة (46 فـ2) من القانون (15– 04) المتعلق بالتوقيع والتصديق الإلكترونيين على أنه: «... **يحتج بالإلغاء تجاه الغير ابتداء من تاريخ النشر، وفقا لسياسة التصديق الإلكتروني لمؤدي خدمات التصديق الإلكتروني**».

من خلال ضمان صحة المعلومات وسريتها، وكذا إثبات مضمون التعامل الإلكتروني عن طريق إصدارها لشهادات التصديق الإلكتروني.

وتكمن الأهمية العملية من وراء تحديد التزامات جهات التصديق الإلكتروني، في تحديد طبيعة المسؤولية التي تقع على عاتق هذه الجهات في حال إخلالها بأحد التزاماتها مما ينجر عنه ضرر للغير أو المتعاقدين معها وهذا ما سيتم تفصيله فيما يلي.

المطلب الثاني

المسؤولية المدنية لمؤدي خدمات التصديق الإلكتروني

يلعب مؤدي خدمات التصديق الإلكتروني دورا مهما في إثبات المعاملات الإلكترونيـــــة، وتستمد هذه الأهمية من أهمية الشهادات التي يصدرها والتي يعتمد عليها ذوي الشأن في إتمام معاملاتهم الإلكترونية؛ فعن طريق شهادات التصديق الإلكتروني يتم التأكد من هوية أطراف المعاملة الإلكترونية وكذا صحة التوقيعات الإلكترونية وسلامة البيانات التي تتضمنها.

إن الثقة التي يمنحها مؤدي خدمات التصديق الإلكتروني لأطراف المعاملــة الإلكترونـــية، عن طريق إصدار شهادات تصديق إلكتروني موصوفة، تحمله فيما بعد المسؤولية المدنية في حال تعويل شخص ما على هذه الشهادة معتقدا أنها تتضمن معلومات صحيحة فيقدم على الالتزام بسببها، ثم يكتشف لاحقا عدم صحة البيانات الواردة فيها، مما يعرضه لأضرار معتبرة بسبب ضخامة قيمة المعاملات والصفقات التجارية التي تتم إلكترونيا.

تُعد مسؤولية مؤدي خدمات التصديق الإلكتروني من أدق المسائل التي تثيرها المعاملات الإلكترونية نظرا لحداثتها، وكما هو متعارف عليه أن المسؤولية عن الأضرار التي تلحق بالغير –بصفة عامة– تُعد من أهم الموضوعات القانونية التي تتعرض لها الأنظمة القانونية وتضع لها قواعد عامة تحكمها **(فرع أول)**. إلا أنه وإلى جانب هذه القواعد العامة، كثيرا ما يتدخل المشرع بالنسبة لحالة خاصة من حالات المسؤولية وذلك لعدم كفاية القواعد العامة لتنظيمها

وضبطهـــا، ويضع لها قواعد وأحكام خاصة بها تخالف فيها الأحكام العامة، سواء فيما تعلق بشروط قيام المسؤولية أو تقييدها، أو مقدار وقيمة التعويض وكيفيته، وهذا ما حدث بالفعل بالنسبة لمسؤولية مؤدي خدمات التصديق الإلكتروني جراء الأضرار التي يلحقونها بالغير **(فرع ثان)**.

الفرع الأول
مسؤولية مؤدي خدمات التصديق الإلكتروني وفقا للقواعد العامة

تنقسم المسؤولية المدنية لمؤدي خدمات التصديق الإلكتروني إلى نوعين، مسؤولية عقدية تفترض عقدا بين صاحب شهادة التصديق الإلكتروني المتضرر ومؤدي خدمات التصديق الإلكتروني، يُفرض على هذا الأخير التزاما بالضمان لمصلحة الأول، نظرا لوجود رابطة عقدية بينهما أساسها العقد الذي يدور حول تقديم خدمات المصادقة الإلكترونية **(أولا)**.

كما يمكن أن يسأل مؤدي خدمات التصديق الإلكتروني، طبقا للقواعد المدنية على أساس المسؤولية التقصيرية، جراء الأضرار التي تمس الغير الذين لا تربطهم به علاقة عقدية المعتمدين على شهادة التصديق خلاف صاحبها **(ثانيا)**.

أولا: المسؤولية العقدية لمؤدي خدمات التصديق الإلكتروني

المسؤولية العقدية بوجه عام؛ هي جزاء لعدم قيام المتعاقد بتنفيذ التزامه، أو تأخره في التنفيذ مما يؤدي إلى إلحاق الضرر بالمتعاقد الآخر[1]، وعليه فلقيام المسؤولية العقدية يفترض وجود عقد صحيح بين الطرف المسؤول والطرف المضرور، وكذا تحقق الضرر الناتج عن الاخلال بالالتزامات المفروضة نتيجة للعقد القائم.

انطلاقا من ذلك، تقوم المسؤولية العقدية بين مؤدي خدمات التصديق الإلكتروني والموقّع نتيجة لعقد صحيح أبرم بينهما، مشتمل على أركانه الثلاث من تراضي صادر من أشخاص ذوي أهلية كاملة خالية من كافة العيوب، ومحل التزام يتعلق بتقديم خدمات التصديق

(1)- فاضلي إدريس، الوجيز في النظرية العامة للالتزام، قصر الكتاب، الجزائر، 2006، ص 144.

بمقابـــل، وكذا توافر سبب يفترض فيه الوجود والمشروعية، وأن يمتنع مؤدي خدمات التصديق الإلكتروني عن تنفيذ هذا العقد أو ينفذه بشكـل معيب ممـــا يسبب ضررا للمُوقـــع، فتتشكل بذلك أركان المسؤولية العقدية والمتمثلة في الخطأ العقدي، الضرر والعلاقة السببية.

1- الخطأ العقدي:

يتحقق الخطأ العقدي لمؤدي خدمات التصديق الإلكتروني بمجرد الاخلال بأحد الالتزامات المفروضة عليه بموجب العقد القائم بينه وبين طالب الخدمة -المُوقّع- ومن بين أهم هذه الأخطاء عدم قيام مؤدي خدمات التصديق الإلكتروني بإصدار شهادة التصديق الإلكتروني المطلوبة منه، أو أن يتأخر في إصدارها، أو أن يصدرها ولكن بشكل معيب؛ كأن تكون قائمة على بيانات غير صحيحة أو مزورة، وكما تعتبر من بين الأخطاء العقدية لمؤدي خدمات التصديق الإلكتروني عدم التزامه بالسرية والحفاظ على البيانات الإلكترونية، أو عدم تعليقه أو إلغائه العمل بشهادات التصديق الإلكتروني في الوقت المحدد وغيرها من الأخطاء التي قد تسبب ضررا للمتعاقد معه[1].

إلا أنه يجب التنبه إلى طبيعة الالتزام الواقع على مؤدي خدمات التصديق الإلكتروني لأجل تحديد الشخص الملزم بإثبات الخطأ أمام القضاء[2]، فإذا كان التزام مؤدي خدمات التصديق الإلكتروني التزاما ببذل عناية، كالتحقق من صحة البيانات المتعلقة بالموقع أو التزامه

---

(1)- كامران الصالحي، الطبيعة القانونية لمسؤولية مزود خدمات التصديق في قانون المعاملات والتجارة الإلكتروني الإماراتي رقم 1 لسنة 2006، مؤتمر المعاملات الإلكترونية (التجارة الإلكترونية-الحكومة الإلكترونية)، مداخلة مقدمة بمركز الإمارات للدراسات والبحوث الإستراتيجية المنعقد في دبي من 19 إلى 20 ماي 2009، ص 651؛ أنظر أيضا: **محمد حاتم البيات**، المسؤولية المدنية عن الخطأ في المعاملات التي تتم عن طريق الوسائط الإلكترونية (التجارة الإلكترونية - الحكومة الإلكترونية) مداخلة مقدمة بمركز الإمارات للدراسات والبحوث الإستراتيجية المنعقد في دبي من 19 إلى 20 ماي 2009، ص 832.

كلتا المداخلتين منشورتين على الموقع التالي: http://www.slconf.uaeu.ac.aeslconf

(2)- عبد الرزاق أحمد السنهوري، الوجيز في النظرية العامة للالتزام، منشاة المعارف للطباعة والنشر والتوزيع، مصر 2004، ص ص 258- 261.

بواجب الاعلام قبل إبرام عقد تقديم الخدمة، ففي هذه الحالة يقع على عاتق المُوقع إثبات أن مؤدي خدمات التصديق الإلكتروني لم يبذل العناية الكافية في تحقيق الالتزام المفروض عليـــه، وتنتفي مسؤولية هذا الأخير بمجرد اثباته أنه بذل العناية اللازمة في أدائه لالتزامه المفروض عليه، وأن الضرر قد وقع لسبب لا يد له فيه.

أما إذا كان التزامه التزاما بتحقيق نتيجة أو غاية كعدم الالتزام بالسرية، أو عدم إصدار شهادة التصديق الإلكتروني أو التأخر في إصدارها، أو عدم تعليق أو إلغاء شهادات التصديق الإلكتروني، ففي هذه الحالة يتحقق الخطأ العقدي بمجرد عدم تحقق النتيجة المطلوبة، ولا يقع على عاتق الموقع إثبات خطأ مؤدي خدمات التصديق الإلكتروني.

2- الضرر:

يعتبر الضرر؛ الركن الثاني الواجب توافره لتحقق المسؤولية العقدية، الذي يستوجب أن يكون العقد قائما وقت حدوثه، وتستبعد من المسؤولية العقدية الأخطاء التي تقع قبل إبرام العقد أو بعد انحلاله[1]، وبالتالي لا يكفي أن يخل مؤدي خدمات التصديق الإلكتروني بأي من التزاماته ليسأل مسؤولية عقدية؛ بل يجب أن يكون هناك ضرر قد لحق بالموقع جراء هذا الإخلال، كأن يفقد الموقّع مفتاحه الخاص ويطلب من مؤدي خدمات التصديق الإلكتروني إلغاء العمل بشهادة التصديق ولم يقم بذلك، ويترتب على ذلك أن يُستعمَل هذا المفتاح من قبل الغير في صفقة باسم صاحب الشهادة، هنا يكون الضرر قد وقع مما يرتب عليه قيام المسؤولية العقدية في مواجهة مؤدي خدمات التصديق الإلكتروني لتعويض صاحب الشهادة عن الضرر الذي لحقه[2].

---

(1)- العربي بلحاج، النظرية العامة للالتزام، ديوان المطبوعات الجامعية، الجزائر، 2001، ص ص 17- 18.

(2)- زهيرة كيسي، النظام القانوني لجهات التوثيق (التصديق) الإلكتروني، دفاتر السياسة والقانون، العدد 07، المركز الجامعي تمنراست، 2012، ص 224.

3- العلاقة السببية:

لا تكفي الأركان السابقة لوحدها لقيام المسؤولية العقدية لمؤدي خدمات التصديق الإلكتروني ما لم تكن هناك علاقة سببية تربط بين الخطأ العقدي والضرر، وعليه تعتبر العلاقة السببية الصلة التي تربط الضرر بالخطأ، فتجعل الضرر نتيجة للخطأ، فإذا انعدمت؛ انتفت المسؤولية لانعدام ركن من أركانها، وتنتفي رابطة السببية عموما إذا تدخل سبب أجنبي يقطع الصلة بين الضرر والخطأ [1].

فالضرر الذي يصيب الموقّع يجب أن يكون سببه الخطأ الذي ارتكبه مؤدي خدمات التصديق الإلكتروني، كأن يصدر شهادة تصديق إلكتروني معيبة مما يؤدي إلى تفويت الصفقة على صاحب الشهادة –المُوقع–، وتعرضه إلى خسارة مادية.

غير أنه يمكن تصور المسؤولية العقدية في إطار العلاقة بين جهة التصديق والغير وفقا لقواعد الاشتراط لمصلحة الغير، ويتحقق ذلك عندما يشترط صاحب التوقيع أن تضمن جهة التصديق تجاه الغير الاضرار التي تحقه نتيجة تعويله على الشهادة، فعندها ينشأ العقد حكما لصالح الغير، إعمالا للقواعد الخاصة بالاشتراط لمصلحة الغير، واستثناء من قاعدة نسبية أثر العقد التي تقصر أحكام العقد والتزاماته على طرفيه [2].

---

(1)- محمد صبري السعدي، شرح القانون المدني الجزائري (مصادر الالتزام – الواقعة القانونية)، ط2، دار الهدى، الجزائر، 2004، ص27.

(2)- إبراهيم الدسوقي أبو الليل، مرجع سابق، ص201.

تنص المادة (116) من القانون المدني الجزائري على أنه: «**يجوز للشخص أن يتعاقد باسمه على التزامات يشترطها لمصلحة الغير، إذا كان له في تنفيذ هذه الالتزامات مصلحة شخصية مادية كانت أو أدبية.**

ويترتب على هذا الاشتراط أن يكسب الغير حقا مباشرا قبل المتعهد بتنفيذ الاشتراط يستطيع أن يطالبه بوفائه، ما لم يتفق على خلاف ذلك، ويكون لهذا المدين أن يحتج ضد المنتفع بما يعارض مضمون العقد.

ويجوز كذلك للمشترط أن يطالب بتنفيذ ما اشترط لمصلحة المنتفع، إلا إذا تبين من العقد أن المنتفع وحده هو الذي يجوز له ذلك».

نشير في الأخير إلى أنه يشترط لاستفادة الغير– الذي يتمثل هنا في الطرف الذي يتعامل بالاستناد على شهادة التصديق– أن تتجه نية طرفي العقد إلى إفادة هذا الغير من العقد، أي أن يضمن مؤدي خدمات التصديق الإلكتروني صحة الشهادة التي أصدرها تجاه هذا الغير.

إضافة إلى قيام المسؤولية العقدية، يمكن أن يسأل مؤدي خدمات التصـــديق الإلكتـروني، طبقا للقواعد المدنية على أساس المسؤولية التقصيرية، جراء الأضرار التي تمس الغير الذين لا تربطهم به علاقة عقدية المعتمدين على شهادة التصديق خلاف صاحبها، وهذا ما سنبينه في النقطة الموالية.

ثانيا: المسؤولية التقصيرية لمؤدي خدمات التصديق الإلكتروني

أوضحنا في النقطة السابقة أن المسؤولية العقدية لمؤدي خدمات التصديق الإلكتروني تغطي الأضرار التي تصيب صاحب الشهادة –الموقّع– وكذا الغير المُشترَط لمصلحته، نظرا لوجود رابطة أساساها العقد الصحيح المرتب لآثاره بين جهة التصديق والموقّع.

أما في حال أن الضرر أصاب شخصا من الغير لم يرتبط بعقد مع مؤدي خدمات التصديق الإلكتروني كما لم يعتبرا مشترطا لصالحه، فإن تطبيق القواعد العامة في القانون المدني تؤدي إلى قيام المسؤولية التقصيرية متى توافر الخطأ والضرر والعلاقة السببية بينها.

تقوم المسؤولية التقصيرية بالاستناد إلى فعل شخصي يحدث ضررا بالغير[1]، فالمسؤولية التقصيرية تعرّف بشكل عام بأنها الحالة التي تنشأ خارج دائرة العقد، ويكون مصدر الالتزام لها هو القانون، فإذا سلك الشخص سلوكا سبب ضررا للغير يلتزم بالتعويض، لذلك فهي تقوم على التزام قانوني واحد وهو عدم الإضرار بالغير.

تنص المادة (124) من القانون المدني الجزائري على أن: **«كل فعل أيا كان يرتكبه الشخص بخطئه، ويسبب ضررا للغير يلزم من كان سببا في حدوثه بالتعويض»**، نلاحظ من خلال هذه المادة؛ أن المشرع الجزائري قد وضع معيار الخطأ كمعيار عام يحكم المسؤولية

(1)- مصطفى العوجي، القانون المدني، ج 2، المسؤولية المدنية، ط 3، منشورات الحلبي الحقوقية، لبنان، 2008، ص 159.

التقصيرية، ووفقا لهذا المعيار فإن كل خطأ يسبب ضـــررا للغير يلـــزم صاحبه بالتعويـــض، وبالتالي يمكن للمسؤولية التقصيرية أن تنشأ عن الفعل الشخصي أو عن فعل الغير أو الأشياء[1].

غير أن إثبات خطأ مؤدي خدمات التصديق الإلكتروني، يعتبر من الأمور الصعبـــة جدا؛ وذلك عائد إلى تشعّب العلاقات الناشئة عن التوقيع الإلكتروني وتنفيذه في منظومة معلوماتية، بالإضافة إلى ذلك، فإن الغير لا يستطيع الدخول إلى البنية التحتية لمؤدي الخدمات، وبالتالي لا يستطيع إثبات الخطأ، لذا فانه في غالب الأحيان ما يتم اللجوء إلى الخبرة القضائية [2].

وعليه، يسأل مؤدي خدمات التصديق الإلكتروني عن فعله الشخصي، كما يمكن أن يسأل عن فعل الغير، ذلك أن مؤدي خدمات التصديق الإلكتروني يستعين أثناء قيامه بمهامه بموارد بشرية ذات كفاءات ومؤهلات عالية في ميدان التصديق الإلكتروني، بحيث تربطهم علاقة تبعية بمؤدي خدمات التصديق الإلكتروني بصفته كمتبوع يمارس السلطة الفعلية في رقابتهم وتوجيههم، ويتحمل مسؤولية أخطائهم، كما تقوم مسؤولية مؤدي الخدمات، بناء على الضرر الذي تحدثه الأشياء غير الحية الموضوعة تحت حراسته، وسنحاول تفصيل كل هذه النقاط فيما سيأتي.

1- مسؤولية مؤدي الخدمات عن فعله الشخصي:

حتى يتحقق قيام المسؤولية التقصيرية وجب على كل متضرر أن يقيم البيّنة على توافر أركانها، وأولها الخطأ التقصيري، أي الاخلال بالتزام قانوني بانحراف الشخص عن السلوك الواجب مع إدراك هذا الانحراف [3]، والالتزام في هذه الحالة هو التزام ببذل عناية وليس بتحقيق نتيجة؛ كأن لا يمارس مؤدي خدمات التصديق الإلكتروني العناية اللازمة لضمان دقة ما يقدمه

---

(1)- محمد صبري السعدي، شرح القانون المدني الجزائري (مصادر الالتزام –الواقعة القانونية)، ط2، دار الهدى، الجزائر، 2004، ص 28.

(2)- محمد رضا أزرو، مرجع سابق، ص 280؛ **المعتصم بالله فوزي أدهم**، مرجع سابق، ص 371.

(3)- محمد صبري السعدي، المرجع نفسه، ص 29.

من تأكيدات ذات صلة بشهادة التصديق، أو كأن يوجب القانون تعليق أو إلغاء شهادة التصديق ويُخِل بهذا الالتزام مما أحدث ضررا للغير الذي عوّل على هذه الشهادة المفروض إلغاؤها أو تعليق العمل بها.

كما يجب على الغير المضرور إثبات أن ثمة ضرر محقق قد أصابه ناجم عن خطأ جهة التصديق، وبذلك يكون قد جمع أركان المسؤولية التقصيرية من خطأ وضرر وعلاقة سببية بينهما.

وإننا نرى أن عبء الإثبات الذي ألقي على عاتق المضرور في هذه الحالة يعتبر إجحافا في حقه، لأن الأمر يتصل بإثبات عمل فني دقيق مما سيعجزه ذلك، فالعلاقة بين الطرفين غير متوازنة، فجهة التصديق الإلكتروني تتمتع بقدرات فنية عالية لا تتوفر في الشخص المضرور مما يمكنها ببساطة إثبات أن الضرر كان لا بد من وقوعه على الرغـــم من عنايتها وحرصـــها، وحتى ولو فرضنا جدلا بقلب عبء الإثبات في هذه الحالة لظَّلَ الغير المتضرر عاجزا عن فهم ومناقشة ما يقدمه الطرف القوي –جهة التصديق– من حجج ووسائل وفنيات للتخلص من الخطأ.

2- مسؤولية مؤدي الخدمات عن أخطاء تابعيه:

يستعين مؤدي خدمات التصديق الإلكتروني أثناء تأدية مهامه بموارد بشرية ذات خبرات عالية في مجال المعلوماتية، وعليه يعتبر مؤدي خدمات التصديق الإلكتروني كمتبوع يمارس سلطة الرقابة والتوجيه على تابعيه في إطار تأدية مهامهم.

بالعودة إلى أحكام نص المادة (136) من القانون المدني الجزائري[1]، نجد أنه لقيام مسؤولية مؤدي خدمات التصديق الإلكتروني عن فعل مساعديه يجب تحقق شرطين أساسين هما:

(1)- تنص المادة (136) من القانون المدني الجزائري على أنه: «يكون المتبوع مسؤولا عن الذي يحدثه تابعه بفعله الضار متى كان واقعا منه في حالة تأدية وظيفته أو بسببها أو بمناسبتها

_ قيام علاقة التبعية بين شخصين أحدهما متبوع والآخر تابع.
_ ارتكاب المتبوع خطأ حال تأدية الوظيفة أو بسببها أو بمناسبتها.

وبتطبيق هذين الشرطين على مؤدي خدمات التصديق الإلكتروني نجد، أن هناك علاقة تبعية بين هذا الأخير وموظفيه أساسها عقد العمل، فمؤدي الخدمات هو من يقوم بتشكيل فريق عمله بكل حرية، ويختار كوادر بشرية تتمتع بمؤهلات عالية تمكنهم من أداء مهامهم، وعليه يمتلك المتبوع هنا –مؤدي الخدمات– سلطة فعلية في إصدار الأوامر وتوجيه ورقابة التابع –المستخدمين–.

أما عن الشرط الثاني، فيكون مؤدي الخدمات مسؤولا عن الفعل الضار المُثبت الذي يرتكبه مستخدميه أثناء تأديتهم لوظيفتهم أو بسببها، فإذا انتفت مسؤولية المستخدم –التابع– إما لسبب عدم ثبوت الخطأ في جانبه، أو لحدوث سبب أجنبي لا يد له فيه؛ انتفت معه مسؤولية مؤدي خدمات التصديق الإلكتروني –المتبوع–.

ويمكن تصور الأخطاء التي قد يقع فيها التابعين لمؤدي خدمات التصديق الإلكتروني كالعمل سهوا على إفشاء المعطيات الشخصية لصاحب الشهادة، أو أن لا يتحقق من هوية صاحب طلب الشهادة عند إيداعه للطلب...

3- مسؤولية مؤدي الخدمات عن الأشياء غير الحية:

إضافة لإمكانية سؤال مؤدي خدمات التصديق الإلكتروني عن الأضرار الناجمة عن فعله الشخصي أو فعل تابعيه، يُمكن أن يسأل أيضا عن الأضرار التي تحدثها الأشياء غير الحية الموضوعة تحت حراسته، وفقا لنص المادة (138) من القانون المدني الجزائري: «**كل من تولى حراسة شيء وكانت له قدرة الاستعمال والتسيير، والرقابة، يعتبر مسؤولا عن الضرر الذي يحدثه ذلك الشيء**.

=**وتتحقق علاقة التبعية ولو لم يكن المتبوع حرا في اختيار تابعه متى كان هذا الأخير يعمل لحساب المتبوع**».

ويعفى من هذه المسؤولية الحارس للشيء إذا اثبت أن ذلك الضرر حدث بسبب لم يكن يتوقعه مثل عمل الضحية، أو عمل الغير، أو الحالة الطارئة، أو القوة القاهرة».

تقوم مسؤولية حارس الشيء بالنسبة لمؤدي خدمات التصديق الإلكتروني، في حال عدم بذله العناية اللازمة في إصلاح منظومة إحداث وفحص التوقيعات الإلكترونية، أو عجز البرامج والمعدات أو الأنظمة المعلوماتية في الإدراج الفوري والإتاحة اللحظية لقوائم الشهادات الملغاة...، وتتحقق هذه المسؤولية بمجرد توافر شرطان، يتعلق الأول بأن تكون حراسة مؤدي خدمات التصديق الإلكتروني لهذه الأشياء غير الحية حراسة فعلية، وأن يتصرف فيها بالاستعمال والتوجيه والرقابة باعتبارها أدوات لتحقيق نشاط التصديق الإلكتروني، أما الشرط الثاني فيتعلق في أن يتسبب الشيء المحروس في إحداث ضرر للغير؛ أي تحقق العلاقة السببية بين الضرر الحاصل وبين تدخل الشيء الإيجابي[1].

يتضح لنا مما سبق؛ أن الأحكام الواردة في القواعد العامة فيما يخص مسؤولية مؤدي خدمات التصديق الإلكتروني، لا تكفي لوحدها لكييف وتحديد نوع المسؤولية، ما استوجب الاستعانة بالقواعد الخاصة المنظمة لخدمات التصديق الإلكتروني، التي من شأنها أن تساعد على تحديد طبيعة المسؤولية المترتبة على كل طرف تربطه أو لا تربطه علاقة عقدية بمؤدي خدمات التصديق الإلكتروني.

الفرع الثاني

مسؤولية مؤدي خدمات التصديق الإلكتروني وفقا للقواعد الخاصة

نظرا لعدم قدرة القواعد العامة للمسؤولية على تنظيمها لمسؤولية مؤدي خدمات التصديق الإلكتروني، قامت معظم التشريعات الدولية والوطنية المنظمة للمعاملات الإلكترونية بوضع قواعد خاصة بمسؤولية مؤدي خدمات التصديق الإلكتروني في حال مخالفتهم للأحكام والقواعد المنظمة لنشاطهم وصلاحياتهم.

---

(1)- دحماني سمير، مرجع سابق، ص 185.

نجد في مقدمة هذه التشريعات قانون اليونسترال النموذجي بشأن التوقيعات الإلكترونية لسنة (2001)، حيث نظم مسؤولية جهات التصديق بناء على الالتزامات المقررة على عاتقهـــا، فبعد أن تضمنت المادة (9)[1] منه مهام والتزامات جهات التصديق نص من خلال الفقرة الأخيرة على مسؤولية جهات التصديق وذلك كما يلي: «... **يتحمّل مقدّم خدمات التصديق التبعات القانونية لتخلّفه عن الوفاء باشتراطات الفقرة1».**

نلاحظ من خلال هذه المادة، أن مسؤولية جهات التصديق تكون مفترضة في حال اخلالها بأحد الالتزامات التي نصت عليها المادة (9 /1) من قانون اليونسترال النموذجي بشأن التوقيعات الإلكترونية لسنة (2001) والمتعلقة أساسا بصحة البيانات الواردة في شهادة

---

(1)- تنص المادة (9) من قانون اليونسترال النموذجي بشأن التوقيعات الإلكترونية لسنة (2001) على: «**حيثما يوّفر مقدّم خدمات التصديق خدمات لتأييد توقيع إلكتروني يجوز استخدامه لإعطاء مفعول قانوني بصفته توقيعا، يتعيّن على مقدّم خدمات التصديق المشار إليه:**

(أ) أن يتصرّف وفقا للتأكيدات التي يقدمها بخصوص سياساته وممارساته؛

(ب) أن يولي قدرا معقولا من العناية لضمان دقة واكتمال كل ما يقدّمه من تأكيدات جوهرية ذات صلة بالشهادة طيلة دورة سريانها، أو مدرجة في الشهادة؛

(ج) أن يوّفر وسائل يكون الوصول إليها متيسّرا بقدر معقول وتمّكن الطرف المعوّل من التأكد، من الشهادة، مما يلي:

1- هويّة مقدّم خدمات التصديق؛'

2-أن الموّقع المعيّنة هويته في الشهادة كان يتحكم في بيانات إنشاء التوقيع في وقت إصدار الشهادة؛

3- أن بيانات إنشاء التوقيع كانت صحيحة في وقت إصدار الشهادة أو قبله؛

(د) أن يوّفر وسائل يكون الوصول إليها متيسّرا بقدر معقول وتمكن الطرف المعوّل من التأكد، عند الاقتضاء، من الشهادة أو من سواها، مما يلي:

1- الطريقة المستخدمة في تعيين هوية الموّقع؛

1- وجود أي تقييد على الغرض أو القيمة التي يجوز أن تُستخدم من أجلها بيانات إنشاء التوقيع أو أن تُستخدم من أجلها الشهادة؛

2-أن بيانات إنشاء التوقيع صحيحة ولم تتعرّض لما يثير الشبهة؛

3- وجود أي تقييد على نطاق أو مدى المسؤولية التي اشترطها مقدّم خدمات التصديق؛

4- ما إذا كانت هناك وسائل متاحة للموّقع لتقديم إشعار بمقتضى الفقرة١ (ب) من المادة ٨ من هذا القانون؛

5- ما إذا كانت تُتا خدمة إلغاء آنيّة؛

(هـ) أن يوّفر، حيثما تُقدم الخدمات بمقتضى الفقرة الفرعية (د/5) وسيلة للموقّع لتقديم إشعار بمقتضى الفقرة (1/ب) من المادة (8) من هذا القانون، وأن يضمن، حيثما تقدّم الخدمات بمقتضى الفقرة الفرعية (د/6) إتاحة خدمة إلغاء آنيّة؛

(و) أن يستخدم في أداء خدماته نظما وإجراءات وموارد بشرية جديرة بالثقة...».

التصديق الإلكتروني أو صحة العلاقة فيما بين الموقع ومفاتيح توقيعه الإلكتروني، وأخيرا الاخلال بالالتزام الخاص بإيقاف أو إلغاء العمل بشهادة التصديق الإلكتروني.

وتنتفي مسؤولية جهة التصديق وفقا للمادة (11) [1] من القانون نفسه ويتحملها الطرف المعول على الشهادة في حال عدم أخذه الاحتياطات اللازمة والمعقولة للتأكد من صحة ومصداقية التوقيع الإلكتروني أو الشهادة، وكذا في حال تجاوزه لحدود الشهادة.

أما عن التنظيم الأوروبي رقم (2014/910) فقد نص من خلال المادة (13) منه على أن: «**مؤدي خدمات الثقة الإلكتروني يكونون مسؤولين عن الأضرار الناجمة عن عمد أو إهمال التي تلحق بأي شخص طبيعي أو معنوي لعدم الوفاء بالالتزامات المفروضة عليهم في هذا التنظيم،**

يتعين على الشخص الطبيعي أو المعنوي مدعي الأضرار اثبات ان مقدم خدمات الثقة غير المؤهل قد تصرف عن عمد أو إهمال،

يفترض في مقدم خدمات الثقة المؤهل الموصوف أنه يتصرف عن عمد أو إهمال، مالم يثبت بأن الأضرار قد حدثت دون إهمال أو قصد من قبله،

عندما يقوم مقدمو خدمات الثقة بإبلاغ عملائهم مسبقا عن القيود الواردة على استخدام خدماتهم التي يقدمونها، وأن تكون هذه القيود واضحة ومفهومة من قبل الغير، لا يمكن تحميل مقدمي خدمات الثقة المسؤولية الناتجة عن الأضرار الناجمة عن تجاوز القيود المشار إليها» [2].

---

(1)– تنص المادة (11) من قانون اليونسترال النموذجي بِشأن التوقيعات الإلكترونية لسنة (2001) على: «**يتحمّل الطرف المعوّل التبعات القانونية الناجمة عن تخلفه عن:**

(أ) اتخاذ خطوات معقولة للتحّقق من قابلية التعويل على التورقيع الإلكتروني؛ أو

(ب) اتخاذ خطوات معقولة، إذا كان التوقيع الإلكتروني مؤيّدا بشهادة،

لأجل:

1- التحّقق من صلاحية الشهادة أو وقفها أو إلغائها؛

2- مراعاة وجود أي تقييد بخصوص الشهادة».

(2)- Article 13 du règlement n° 910-2014: «**1. Sans préjudice du paragraphe 2, les prestataires de services de confiance sont responsables des dommages causés intentionnellement ou par négligence à toute personne physique ou morale en raison d'un manquement aux obligations prévues par le présent règlement.**

Il incombe à la personne physique ou morale qui invoque les dommages visés au premier alinéa de prouver que le prestataire de services de confiance non qualifié a agi intentionnellement ou par négligence.

من خلال القراءة الأولية لهذه المادة نجد، أن المشرع الأوروبي قد أقام مسؤولية مقدمي خدمات الثقة عن الاخلال بأي من الالتزامات الواقعة عليه دون تفصيل منه لماهية الحالات التي تؤدي إلى قيام مسؤوليته.

كما أنه ميز بين حالتين بشأن افتراض مسؤولية مقدم خدمات الثقة؛ حيث أنه أقر المسؤولية المفترضة في جانب مقدم خدمات الثقة الموصوف، فافترض أن تصرفه قائم عن عمد أو إهمال ما لم يثبت بأن الأضرار قد وقعت دون إهمال أو قصد منه، في حين لم يطبق أحكام المسؤولية المفترضة على مقدم خدمات الثقة غير الموصوف، بل ألزم الشخص الطبيعي أو المعنوي المتضرر من إثبات خطأ مقدم خدمات الثقة غير الموصوف وفقا للقواعد العامة.

أما عن الفقرة الأخيرة من المادة فقد أقرت تقييد مسؤولية مقدم خدمات الثقة عن الأضرار التي قد تحدث للغير في حال تجاوزهم للقيود المحددة في العقد المبرم بينهم، كتجاوز الحد الأقصى لقيمة المعاملات المحددة في الشهادة، أو استعمالها بعد نهاية صلاحيتها، ففي هذه الحالة لا يمكن مساءلة مقدم خدمات الثقة عن الأضرار اللاحقة بالغير بشرط ان تكون هذه القيود واضحة ومفهومة من قبل الغير.

إضافة إلى ما سبق، يعفى مقدم خدمات الثقة من المسؤولية في حال إثباته أن الضرر قد وقع دون قصد أو إهمال من طرفه، بل بسبب إما الطرف الآخر أو بسبب أجنبي لا يد له فيه.

أما بالنسبة للمشرع الفرنسي فقد فضل التطرق لحالات قيام مسؤولية مقدم خدمات الثقة بموجب المادة (33)[1] من القانون الفرنسي رقم (2004-575) بشأن الثقة في الاقتصاد

Un prestataire de services de confiance qualifié est présumé avoir agi intentionnellement ou par négligence, à moins qu'il ne prouve que les dommages visés au premier alinéa ont été causés sans intention ni négligence de sa part.

2. Lorsque les prestataires de services de confiance informent dûment leurs clients au préalable des limites qui existent à l'utilisation des services qu'ils fournissent et que ces limites peuvent être reconnues par des tiers, les prestataires de services de confiance ne peuvent être tenus responsables des dommages découlant de l'utilisation des services au-delà des limites indiquées.

3. Les paragraphes 1 et 2 s'appliquent conformément aux règles nationales en matière de responsabilité ».

(1)-Article 33 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique:« **Sauf à démontrer qu'ils n'ont commis aucune faute intentionnelle ou négligence, les prestataires de services de certification électronique sont responsables du préjudice causé aux personnes qui se sont fiées raisonnablement aux certificats présentés par eux comme qualifiés dans chacun des cas suivants :**

1° Les informations contenues dans le certificat, à la date de sa délivrance, étaient inexactes ;

الرقمي سالف الذكر، والتي اعتبرت أن مقدم خدمات الثقة مسؤولا مسؤولية مفترضة في حال لحق ضرر بالأشخاص المعولين على شهادات التصديق الموصوفة الصادرة عنه مالم يُقِم الدليل على أنه لم يرتكب أي خطأ عمدي أو إهمال من طرفه، وذلك في الحالات التالية:

- عدم دقة المعلومات الواردة في الشهادة في تاريخ صدورها،
- عدم اكتمال البيانات المطلوبة لاعتبار شهادة التصديق موصوفة،
- لم يؤد إصدار الشهادة إلى التحقق من أن المفتاح الخاص للموقع يناظر المفتاح العام،
- لم يقم مقدم خدمات الثقة عند الاقتضاء بإجراء إلغاء الشهادة، وظلت المعلومات تحت تصرف الغير.

وكباقي التشريعات التي بيناها سابقا يُعفى مؤدي خدمات التصديق الإلكتروني الفرنسي من المسؤولية في حال تجاوز الطرف المعول على الشهادة القيود الموضوعة على استخدامها أو قيمة المعاملات المحددة فيها، شريطة أن تكون هذه القيود واضحة ومفهومة للغير.

في حين أن المشرع التونسي قد تناول مسؤولية مزود خدمات التوثيق الإلكتروني من خلال الفصل (22)[1] من قانون المبادلات والتجارة التونسي (83 لسنة 2000)، إذ حَمَّل مزود

2° Les données prescrites pour que le certificat puisse être regardé comme qualifié étaient incomplètes ;
3° La délivrance du certificat n'a pas donné lieu à la vérification que le signataire détient la convention privée correspondant à la convention publique de ce certificat ;
4° Les prestataires n'ont pas, le cas échéant, fait procéder à l'enregistrement de la révocation du certificat et tenu cette information à la disposition des tiers.
Les prestataires ne sont pas responsables du préjudice causé par un usage du certificat dépassant les limites fixées à son utilisation ou à la valeur des transactions pour lesquelles il peut être utilisé, à condition que ces limites figurent dans le certificat et soient accessibles aux utilisateurs.
Ils doivent justifier d'une garantie financière suffisante, spécialement affectée au paiement des sommes qu'ils pourraient devoir aux personnes s'étant fiées raisonnablement aux certificats qualifiés qu'ils délivrent, ou d'une assurance garantissant les conséquences pécuniaires de leur responsabilité civile professionnelle ».

(1)- ينص الفصل (22) من قانون المبادلات والتجارة الإلكترونية التونسي (83 لسنة 2000) على أنه: **«يكون مزود خدمات المصادقة الإلكترونية مسؤولا عن كل ضرر حصل لكل شخص وثق عن حسن نية في الضمانات المنصوص عليها بالفصل 18 من هذا القانون.**

ويكون مزود خدمات المصادقة الإلكترونية مسؤولا عن الضرر الحاصل لكل شخص نتيجة عدم تعليق أو إلغاء الشهادة طبقا للفصلين 19 و20 من هذا القانون. =

خدمات التوثيق مسؤولية الأضرار اللاحقة بالطرف المعول على شهادة التصديق الإلكتروني نتيجة إخلاله بالالتزامات المفروضة عليه بموجب الفصل (18) من القانون نفسه، والمتعلقة أساسا ب:

- عدم ضمان صحة المعلومات الواردة في الشهادة وقت إصدارها،
- عدم مطابقة بيانات إحداث التوقيع الإلكتروني مع بيانات فحصه،
- عدم التدقيق في المعلومات المقدمة إليها في طلبات إصدار شهادات التصديق الإلكتروني.

إضافة إلى ذلك، تقوم مسؤولية مزود خدمات التوثيق الإلكتروني في حال إخلاله بالالتزامات المفروضة عليه وفقا للفصلين (19) و(20) من القانون نفسه، والخاصة بتعليق العمل بالشهادة أو إلغائها في حال توافر الأسباب الجدية الموجبة لذلك والتي بيّانها سابقا.

في حين أعفت الفقرة الأخيرة من الفصل (22) مزود خدمات الثقة من مسؤوليته في حال تم إثبات أن الضرر ناجم عن عدم احترام صاحب الشهادة لشروط استعمالها أو شروط إحداث إمضائه الإلكتروني.

كذلك الحال بالنسبة للمشرع المغربي فقد نص في المادة (2/24) من القانون (05-53) المتعلق بالتبادل الإلكتروني للمعطيات القانونية سالف الذكر، على أن مقدمي خدمات المصادقة الإلكترونية: «...**يتحملون وفق القواعد القانونية العادية، مسؤولية تهاونهم أو قلة كفاءتهم أو قصورهم المهني سواء تجاه المتعاقدين معهم أو تجاه الأغيار...**»

وعليه حمل المشرع المغربي من خلال هذه المادة مقدمي خدمات المصادقة الإلكترونية المسؤولية وفقا للقواعد العامة في حال إخلالهم بالالتزامات المفروضة على عاتقهم، وفي هذه الحالة يقع عبء إثبات الخطأ على الطرف المضرور.

=لا يكون مزود خدمات المصادقة الإلكترونية مسؤولا عن الضرر الناتج عن عدم احترام صاحب الشهادة لشروط استعمالها أو شروط إحداث إمضائه الإلكتروني».

وعلى غير العادة لم يول المشرع المصري اهتماما بتنظيم مسؤولية مزود الخدمات بموجب نصوص خاصة على الرغم من أهمية الموضوع، إذ لم يتطرق من خلال القانون (15 لسنة 2004) إطلاقا إلى مسؤولية مزود الخدمات، إلا أنه أشار إليها بشكل ضمني في لائحته التنفيذية لقانون التوقيع الإلكتروني لسنة (2005) إذ تنص المادة (14) منه على أن: «**على طالب الترخيص بإصدار شهادات التصديق الإلكتروني أن يقدم الضمانات والتأمينات التي يحددها مجلس إدارة الهيئة لتغطية أي أضرار أو أخطار تتعلق بذوي الشـــأن، وذلك في حال إنهاء الترخيص لأي سبب، أو لتغطية أي إخلال من جانبه لالتزاماته الواردة في الترخيص**».

أما عن المشرع الجزائري فقد نظم هذه المسؤولية في القسم الثاني من الفصل الثالث من القانون رقم: (15- 04) المتعلق بالتوقيع والتصديق الإلكترونيين سالف الذكر، بموجب المواد من (53) إلى (57)[1]؛ إذ نص على أن مؤدي خدمات التصديق الإلكتروني يتحمل المسؤولية

---

(1)- تنص المادة (53) من القانون (15- 04) على أن: «**يكون مؤدي خدمات التصديق الإلكتروني الذي سلم شهادة تصديق الكتروني موصوفة، مسؤولا عن الضرر الذي يلحق بأي هيئة أو شخص طبيعي أو معنوي، اعتمد على شهادة التصديق الإلكتروني هذه، وذلك فيما يخص:**

1- صحة جميع المعلومات الواردة في شهادة التصديق الإلكتروني الموصوفة، فـــي التاريـخ الذي منحـــت فيـــه، ووجود جميع البيانات الواجب توفرها في شهادة التصديق الإلكتروني الموصوفة ضمن هذه الشهادة،

2- التأكد عند منح شهادة التصديق الإلكتروني، أن الموقع الذي تم تحديد هويته في شهادة التصديق الإلكتروني الموصوفة، يحوز كل بيانات إنشاء التوقيع الموافقة لبيانات التحقق من التوقيع المقدمة و/أو المحددة في شهادة التصديق الإلكتروني،

3- التأكد من إمكانية استعمال بيانات إنشاء التوقيع، والتحقق منه بصفة متكاملة.

إلا في حالة ما إذا قدم مؤدي خدمات التصديق الإلكتروني ما يثبت انه لم يرتكب أي إهمال».

- تنص المادة (54) من القانون (15- 04) على أنه: «**يكون مؤدي خدمات التصديق الإلكتروني الذي سلم شهادة تصديق إلكتروني موصوفة، مسؤولا عن الضرر الناتج عن عدم إلغاء شهادة التصديق الإلكتروني هذه، والذي يلحق بأي هيئة أو شخص طبيعي أو معنوي اعتمدوا على تلك الشهادة، إلا إذا قدم مؤدي خدمات التصديق الإلكتروني ما يثبت انه لم يرتكب أي إهمال**».

- تنص المادة (55) من القانون (15- 04) على أنه: «**يمكن مؤدي خدمات التصديق الإلكتروني أن يشير، في شهادة التصديق الإلكتروني الموصوفة، إلى الحدود المفروضة على استعمالها، بشرط أن تكون هذه الإشارة واضحة ومفهومة من طرف الغير.**

=

المدنية الناتجة عن الضرر اللاحق بالطرف المعوّل على شهادة التصديق الإلكتروني الموصوفة، نتيجة عدم صحة البيانات الواردة في الشهادة وقت إصدارها، أو عدم مطابقة بيانات إنشاء التوقيع الإلكتروني مع بيانـات فحصــه، أو إخلاله بالتزام إلغاء الشهادة بعد ثبوت دواعي ذلك.

تنتفي مسؤولية مؤدي خدمات التصديق الإلكتروني في حال إثباته أنه لم يرتكب أي إهمال، أو في حال تجاوز الموقّع حــدود استعمــال الشهــادة أو القيمة المحددة فيها وفقا لما نصت عليه المادتين (55) و(56) سالفتي الذكر. حيث أقام المشرع الجزائري نوعا من التوازن بين مصالح مؤدي خدمات التصديق الإلكتروني والغير الذي يعتمد على هذه الشهادة، بإعطائه الصلاحية لمؤدي خدمات التصديق الإلكتروني لتحديد نطاق صلاحية الشهادة، بحيث لا يمكن مساءلته في حال تجاوز هذا النطاق، وتحديد نطاق الشهادة يمس كل من قيمة ونوع المعاملات، حيث حدد نوع المعاملات التي تتضمنها الشهادة.

من خلال ما تم التطرق إليه بخصوص مسؤولية مؤدي خدمات التصديق الإلكتروني نتوصل إلى أن أحكام المسؤولية المدنية العامة سواء العقدية أو التقصيرية هي المرجع الأساسي لقيام مسؤولية مؤدي خدمات التصديق الإلكتروني بالرغم من استحداث نصوص قانونية خاصة لتنظيم هذه المسؤولية، إلا أنه عند استقراء هذه النصوص نجدها مستمدة أساسا من القواعد العامة للمسؤولية المدنية كحالات الإعفاء أو تقييد مسؤولية مؤدي الخدمات.

=وفي هذه الحالة، لا يكون مؤدي خدمات التصديق الإلكتروني مسؤولا عن الضرر الناتج عن استعمال شهادة التصديق الإلكتروني الموصوفة، عند تجاوز الحدود المفروضة على استعمالها».

- تنص المادة (56) من القانون (15- 04) على أنه: **«يمكن مؤدي خدمات التصديق الإلكتروني، أن يشير في شهادة التصديق الإلكتروني الموصوفة، إلى الحد الأقصى لقيمة المعاملات التي يمكن أن تستعمل في حدودها هذه الشهادة، بشرط أن تكون هذه الإشارة واضحة ومفهومة من طرف الغير. وفي هذه الحالة، لا يكون مؤدي خدمات التصديق الإلكتروني مسؤولا عن الضرر الناتج عن تجاوز ذلك الحد الأقصى».**
- تنص المادة (57) من القانون (15- 04) على أنه: **«لا يكون مؤدي خدمات التصديق الإلكتروني مسؤولا عن الضرر الناتج عن عدم احترام صاحب شهادة التصديق الإلكتروني الموصوفة لشروط استعمال بيانات إنشاء التوقيع الإلكتروني».**

كما يتضح أيضا أن هذه النصوص قد تطرقت إلى نقاط عامة تتعلق أساسا بالإخلال بالالتزامات المفروضة على عاتق مؤدي خدمات التصديق، في حين أنها لم تتطرق بالتنظيم إلى نقاط أكثر خصوصية كتلك المتعلقة بالقانون الواجب التطبيق على النزاعات التي تثور بين مؤدي خدمات التصديق والمتعاملين معه، وكذا الجهة القضائية المختصة بالفصل في النزاعات خصوصا في حال وجود طرف أجنبي في العلاقة.

ما لاحظناه كذلك عدم تنظيم المشرع الأردني لكل ما يتعلق بجهات التصديق الإلكتروني بدءا بالالتزامات وصولا للمسؤولية، ولعل إغفال المشرع الأردني تنظيم هذه المسألة هدفه إخضاع مسؤولية هذه الجهات لأحكام المسؤولية المدنية وفقا للقواعد العامة.

إن تقرير حماية تقنية لكل من المحررات والتواقيع الإلكترونية لا تكف وحدها لمجابهة المخاطر التي تحيط بها خصوصا في ظل بيئة إلكترونية لا مادية قد تتعرض لشتى أنواع التعدي والاختراق، لذا كان من الضروري التدخل من جديد لحمايتهما من كل أشكال الاعتداء والممارسات غير المشروعة التي قد تتعرض لها البيانات والأنظمة المعلوماتية، لكن هذه المرة بتقرير حماية جزائية تجرم كل صور المساس أو الإضرار بالأنظمة المعلوماتية والمعطيات المتضمنة لها بما فيها تلك المتعلقة بالمحررات والتواقيع الإلكترونية وهذا ما سيأتي تفصيله من خلال الفصل الموالي من هذه الأطروحة.

الفصل الثاني
الحماية الجزائية لأدلة الإثبات الإلكتروني

لا تقتصر مواجهة المخاطر التي قد تمس بأدلة الإثبات الإلكتروني على توفير الحماية الوقائية؛ أو ما يطلق عليها بالحماية التقنية أو الفنية؛ بل وجب أن يكون هذا النظام الأمني مدعما بنظام قانوني واضح المعالم، يتكفل بحماية المحرر والتوقيع في الشكل الإلكتروني من جميع صور المساس بهما، والتصرفات غير المشروعة التي ينجم عنها التعرض لبياناتهما وللأنظمة المعلوماتية التي تتضمنهما، ولا يتأتى ذلك إلا عن طريق إضفاء حماية جزائية للمعاملات الإلكترونية تتصدى لجميع أشكال الاعتداء والجرائم التي قد تقع عليها.

خاصة وأن الجريمة المعلوماتية[1] قد اتخذت صورا عديدة استوجبت معها المواجهة التشريعية تبعاً لآثارها الوخيمة على الفرد والمجتمع، وهذا انطلاقاً من النمط التقليدي للجرائم التي وجدت تطبيقاً حديثاً لها في حيّز المعاملات الإلكترونية الاقتصادية بشكل خاص، بحيث ظهرت بعض الأساليب الحديثة المُشكلة للجرائم الواقعة على الأموال، أو الجرائم الماسة بالثقة في بيئة غير مادية- افتراضية-. يدفعنا للبحث في القواعد العامة للحماية الجزائية من هذه الجرائم وإسقاط أركان الجريمة في صورتها التقليدية على صورتها الإلكترونية **(مبحث أول)**.

---

(1)- عرف المشرع الجزائري الجريمة المعلوماتية بداية بالقانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها من خلال المادة 2 منه بأنها: **«الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية»**. ليوسّع بعد ذلك في هذا التعريف من خلال الأمر رقم 21-11 المؤرخ في 16 محرم عام 1443 الموافق 25 غشت سنة 2021، يتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، من خلال المادة 2 منه باستحداث باب سادس عنوانه: " القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، حيث نص من خلال المادة 211 مكرر 22 ف 2: **«... يقصد بمفهوم هذا القانون، بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، أي جريمة ترتكب أو يسهل ارتكابها استعمال منظومة معلوماتية أو نظام للاتصالات الإلكترونية أو أي وسيلة أخرى أو آلية ذات صلة بتكنولوجيات الإعلام والاتصال»**.

كما قد أخذت الجريمة طابعاً نابعاً من طبيعة التعامل الإلكتروني، فبرز نوع مستحدث من الجرائم أخذ قوامه من خلال نطاق المعاملات الإلكترونية وآليات نشوئها وتنفيذها، وهو ما يظهر بدقة في الجرائم الماسة بالنظام المعلوماتي، وكذا الأنشطة الإجرامية التي تمس مضمون التعاملات الإلكترونية كأساليب التعدي على نظام التوقيع الإلكتروني؛ الذي يعد أهم آليات تنفيذ هذا النوع من المعاملات، والذي يرتبط بدوره بشكل مباشر بتحديد مصداقية الأداء للأعمال الإلكترونية، ومدى حجيتها القانونية **(مبحث ثان)**.

إن الإجرام المعلوماتي المتميّز بذات خصائص التقنية المرتكب من خلالها، دفع المشرع الجزائري لأن يحاول تكريس مواجهة جنائية –موضوعية واجرائية– جديدة يسد بها الطريق أمام مجرمين استغلّوا التطوّرات التقنية في تطوير أساليبهم الإجرامية. لذا قام بتعديلات قانونية وكذا إصدار نصوص قانونية أراد من خلالها أن يجسّد إطار قانوني لمواجهة الجرائم المعلوماتية أو على الأقل بجعل القواعد القانونية الموجودة مرنة مرونة تسمح بمواكبة التطوّرات الحاصلة في الفكر الإجرامي الذكي المستحدث.

غير أن دراستنا في هذا الفصل، سترتكز فقط على الجوانب الموضوعية للحماية الجزائية لأدلة الإثبات الإلكتروني في التشريع الجزائري، دون الجوانب الإجرائية لهذه الحماية، خاصة أن كلا الجانبين حديثين ويتضمنان العديد من التفاصيل التي تستلزم التطرق لدراستها، مما لا يسعنا الالمام بهما من خلال هذا الفصل.

المبحث الأول

الحماية الجزائية لأدلة الإثبات الإلكتروني في إطار الجرائم التقليدية

إن التطور التكنولوجي الذي أثّر بشكل إيجابي على مجال المعاملات بين الأفراد وجعلها تتسم بشكل إلكتروني يتميز بالسرعة في الإنجاز ونقص في التكاليف، أثر كذلك بشكل سلبي مس الجانب الإجرامي، حيث أعطى منحى جديد للجرائم عرفت بالجرائم المعلوماتية، أين ارتبط مفهومها ارتباطا وثيقا بالتطور التكنولوجي وتقنية المعلومات.

وبناء عليه، أضحت المعاملات الإلكترونية مجالا خصبا لظهور أشكال عديدة من الاعتداءات التي استلزمت تدخلا تشريعيا لمجابهتها، حيث ظهرت بعض الجرائم الحديثة انطلاقا من النمط التقليدي للجرائم، كالجرائم الواقعة على الأموال في البيئة الإلكترونية؛ مثل السرقة والنصب والاحتيال وخيانة الأمانة، أو الجرائم الماسة بالثقة؛ كجريمة تزوير المحررات الإلكترونية.

من هنا كانت مسألة البحث في قواعد الحماية الجنائية من هذه الجرائم، إسقاطا لشروط وأركان الجريمة في وجهها التقليدي على المجال أو الحيز اللامادي في التعامل الإلكتروني، والخروج بأحكام تتناسب وطبيعة قيام النشاط الإجرامي، وفرض الجزاء المناسب له، بالموازاة مع عدم الخروج عن القواعد والمبادئ التي يقوم عليها الحكم التشريعي الجنائي؛ وعلى رأسها مبدأ المشروعية.

وعليه، سنحاول من خلال هذا المبحث التطرق إلى جريمة التزوير الإلكتروني كنموذج عن الجرائم الماسة بالثقة **(مطلب أول)**، ثم جريمة السرقة المعلوماتية كنموذج عن الجرائم الماسة بالأموال **(مطلب ثان)**، لنبين من خلال هذا المبحث مدى إمكانية استيعاب النصوص التقليدية للجرائم الإلكترونية.

المطلب الأول
جريمة التزوير الإلكتروني

على الرغم من الحماية التقنية المقررة للمحررات والتواقيع الإلكترونية التي كرستها تشريعات الإثبات الإلكتروني، إلا أن هذا الأمر لم يمنع المجرمين من تذليل هذه التقنيات لحل الشفرات والاطلاع على محتواها وكذا تغيير الحقيقة فيها بشكل يسبب ضررا للغير، لتضاف لعالم الجرائم جريمة التزوير الإلكتروني.

تعد جريمة التزوير الإلكتروني إحدى أهم الجرائم الإلكترونية، لما لها من تهديد للثقة العامة للمتعاملين بالمحررات الإلكترونية محل جريمة التزوير، وما لها من إخلال باستقرار المعاملات الإلكترونية التي تتم عن طريقها، فآثارها لا تقتصر فقط على الأفراد، أو في إطار محلي محدود، بل على مستوى واسع وفي فضاء دولي مفتوح، كما أن سرعة تطورها وازدياد حجمها جعل منها محل اهتمام أغلب النظم التشريعية الحديثة.

للإحاطة بدراسة هذه الجريمة ارتأينا تقسيم هذا المطلب إلى فرعين، إذ نبين مفهوم هذه الجريمة من خلال التطرق إلى التعريفات المقدمة لها وكذا الخصائص التي تتميز بها **(فرع أول)** لنتطرق فيما بعد للبناء القانوني لهذه الجريمة من خلال التطرق لأركانها وكيفية المعالجة التشريعية لها **(فرع ثان)**.

الفرع الأول
مفهوم جريمة التزوير الإلكتروني

يتميز التزوير الواقع على أدلة الإثبات الإلكتروني بسهولته وبساطته عن ذلك الذي يقع على أدلة الإثبات التقليدي، كون أن التزوير في محرر إلكتروني لا يحتاج إلى استخدام الأدوات والمواد الكيماوية لتغيير الكلمات أو كشط التوقيعات، بل كل ما يحتاجه إدخال أو تغيير معاني كلمات بالحذف أو الإضافة أو التعديل عليها، وبذلك ينتج محرر أصلي على الرغم من تزوير مضمونه.

تتميز جريمة التزوير بصفة؛ عامة والتزوير الإلكتروني بصفة خاصة؛ بالتعقيد نظرا لاتصالها بالثقة العامة والتي من شأنها إحداث ضرر بالحقوق أو بالمراكز القانونية لأطراف المحرر الإلكتروني المزور، لذا كان لزاما على الدول ضبطها وتحديد مفهوم عام مشترك لهذه الجريمة **(أولا)**، مع ضرورة إبراز خصائصها وما يميزها عن جريمة التزوير التقليدي **(ثانيا)**.

أولا: تعريف التزوير الإلكتروني

استقر بعض الفقه على تعريف التزوير في المحررات بصفة عامة على أنه: **«عملية وصورة من صور الكذب التي يقوم بها الشخص بغرض تغيير الحقيقة بقصد الغش في محرر عمومي أو رسمي بإحدى الطرق المادية أو المعنوية المقررة قانونا، ومن شأنه إلحاق الضرر بالحقوق أو المراكز القانونية لأحد أو بعض أطراف السند أو المحرر محل الادعاء بالتزوير، مع توافر نية استعمال المحرر فيما يزور من أجله»** [1].

وقد عرفه الفقيه "**EMILE Garçon**" بأنه: **«تغيير الحقيقة بقصد الغش في محرر بإحدى الطرق التي نص عليها القانون تغييرا من شأنه أن يسبب ضررا»** [2].

غير أنه وبعد التطور التكنولوجي اكتسب التزوير شكلا جديدا وأضحى يطلق عليه "التزوير الإلكتروني"؛ وذلك لوروده على المحررات الإلكترونية، وقد حاول الفقه توسيع المفهوم التقليدي للتزوير ليشمل التزوير الإلكتروني، إذ عرفه البعض منهم بأنه: **«تغيير للحقيقة في المستندات المعالجة آليا والمستندات المعلوماتية وذلك بنية استعمالها»** [3].

كما يُعرف التزوير الإلكتروني أيضا بأنه: **«تغيير للحقيقة بأي وسيلة كانت سواء كان ذلك في محرر أو دعامة طالما أن هذه الدعامة ذات أثر في إنشاء حق، أو لها شأن في**

---

(1)–**عبد العزيز سعد**، جرائم التزوير وخيانة الأمانة واستعمال المزور، دار هومة، الجزائر، 2005، ص 14؛ **محمد حسين علي محمود**، التزوير باستخدام الوسائل الإلكترونية، رسالة ماجستير في الحقوق، كلية الحقوق، جامعة القاهرة، 2011، ص 36.

(2)– **نبيل صقر**، الوسيط في الجرائم المخلة بالثقة العامة، دار الهدى، الجزائر، 2015، ص 190.

(3)– **علي عبد القادر القهوجي**، الحماية الجنائية للبيانات المعالجة إلكترونيا، بحث مقدم لمؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، الإمارات العربية المتحدة، 1–3 ماي 2000، ص 63.

إحداث نتيجة معينة»[1]، كما اعتبره جانب آخر من الفقه بأنه: **«تغيير للحقيقة في البيانات أو المعلومات المعالجة عن طريق الحاسب الآلي، والتي أصبح لها كيان مادي ملموس يقابل أصل المحرر المكتوب»** [2].

أما عن التعريف التشريعي للتزوير الإلكتروني، فنجد التعريف الذي تعرضت له الاتفاقية الأوروبية لمكافحة الجريمة المعلوماتية "اتفاقية بودابست" الموقعة في (23 نوفمبر 2001) [3]، حيث نصت على التزوير المعلوماتي من خلال المادة (7) كالآتي: **«على كل طرف أن يتخذ من التدابير التشريعية أو أي تدابير أخرى للتجريم وفقا لقانونه الداخلي، الإدخال غير المصرﻫ به، التغيير، المسح أو الحذف بشكل عمدي وبدون حق للمعطيات المعلوماتية، لترتيب معطيات غير موثوق فيها، سواء كانت مقروءة ومفهومة بشكل مباشر أم لا...»** [4].

---

(1)- أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي "دراسة مقارنة"، دار النهضة العربية، ط1، مصر، 2000، ص 407.

ويؤكد الأستاذ "أحمد حسام طه تمام" على أن التزوير يجب أن يتم على مخرجات الحاسب الآلي، وهي المعلومات التي انفصلت عن النظام وأخرجت من الحاسب الآلي في شكل طباعة مكتوبة، أو في شكل تسجيلي على دعامة إلكترونية. أما المعلومات التي يتضمنها نظام المعالجة الآلية للمعطيات؛ أي المسجلة في ذاكرة النظام والتي تُعد جزءا منه؛ فإن الاعتداء عليها بالتلاعب سواء بإدخال معلومات عليها أو تعديلها أو حذفها لا يشكل جريمة التزوير الإلكتروني. لمزيد من التفصيل أنظر: **أحمد حسام طه تمام**، المرجع نفسه، ص 357.

(2)- عبد الفتاﻫ بيومي حجازي، الحكومة الإلكترونية، الكتاب الثاني، دار الفكر الجامعي، مصر، 2008، ص180.

(3)- تم اعتماد الاتفاقية وتقريرها التفسيري من قبل لجنة وزراء مجلس أوروبا في دورتها (109) بتاريخ (23 نوفمبر 2001)، تهدف هذه الاتفاقية بشكل أساسي إلى مواءمة عناصر القانون الموضوعي الجنائي المحلي والأحكام المتصلة بالجرائم في مجال الجريمة الإلكترونية، وكذا التنصيص على صلاحيات القانون الإجرائي الجنائي الداخلي اللازمة للتحقيق في هذه الجرائم ومتابعتها قضائيا، علاوة على الجرائم الأخرى التي ترتكب عن طريق نظام الكومبيوتر أو التي تكون الأدلة المتصلة بها في شكل إلكتروني، إضافة إلى إنشاء نظام سريع وفعال للتعاون الدولي.

تتضمن الاتفاقية على 48 مادة مقسمة على 4 فصول. لمزيد من التفصيل راجع التقرير التفسيري لاتفاقية بودابست.

https://rm.coe.int/explanatory-report-budapest-convention-in-arabic

(4)- Article 7: Convention sur la cybercriminalité : « **Falsification informatique : « Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'introduction, l'altération, l'effacement ou la suppression intentionnels et sans droit de données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles…».** https://www.europarl.europa.eu/

واعتبر التقرير التفسيري للاتفاقية أعلاه بأن حكم هذه المادة يغطي البيانات المكونّة لوثيقة عامة أو خاصة، والتي تترتب عنها آثار قانونية. ويُسفر "الإدخال" غير المرخص لبيانات صحيحة أو خاطئة عن حالة مطابقة لصناعة وثيقة مزّورة. وبشكل عام، تعتبر التغييرات اللاحقة (التعديلات، والاختلافات، والتغييرات الجزئية)، والإتلاف (إعاقة، إخفاء البيانات) بمثابة تزوير وثيقة أصلية[1].

أما عن المشرع الفرنسي فقد اعتمد توسيع مفهوم التزوير التقليدي ليشمل بذلك المحررات الإلكترونية إلى جانب المحررات التقليدية، ذلك من خلال تعديل قانون العقوبات الفرنسي لسنة (1992) بموجب القانون (92-1336)[2]، حيث نص من خلال المادة (441-1) منه على مفهوم واسع للتزوير واعتبره: **«يشكل تزويرا كل تغيير بطريق الغش للحقيقة، من شأنه أن يسبب ضررا، ويرتكب بأي وسيلة كانت في محرر مكتوب أو أي دعامة أخرى للتعبير عن الفكر، يكون الغرض منه إثبات حق أو واقعة لها آثار قانونية»**[3].

وعليه؛ ووفقا لهذه المادة، نلاحظ أن المشرع الفرنسي قد قام بتوسيع مفهوم التزوير ليشمل أي صورة للتعبير عن الفكر؛ تقليدية كانت أو إلكترونية؛ أو حتى ما يمكن أن يُنتجه العلم مستقبلا. كما أنه لم يحدد طريقة معينة لارتكاب التزوير، وهذا معناه إمكانية استخدام شتى الطرق والأساليب المعلوماتية أيا كانت لارتكاب الفعل الجرمي المتمثل في التزوير الإلكتروني[4]، محاولا بذلك استيعاب ما قد تسفر عنه التطورات التكنولوجية في المجال مستقبلا.

---

(1)- راجع في هذا التقرير التفسيري لاتفاقية بودابست، ص 14.
https://rm.coe.int/explanatory-report-budapest-convention-in-arabic

(2)- Loi n° 92-1336 du 16 décembre 1992 relative à l'entrée en vigueur du nouveau code pénal et à la modification de certaines dispositions de droit pénal et de procédure pénale rendue nécessaire par cette entrée en vigueur. https://www.legifrance.gouv.fr/

(3)-Article 441-4 du code pénal français**: «Constitue un faux toute altération frauduleuse de la vérité, de nature à causer un préjudice et accomplie par quelque moyen que ce soit, dans un écrit ou tout autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques**». Modifié par Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002.

(4)- براهيمي حنان، جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية، أطروحة مقدمة لنيل شهادة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، 2015/2014، ص 168.

وهو تقريبا نفس التعريف الوارد في الفصل (172) الفقرة الأخيرة من المجلة الجنائية التونسية، حيث أن العقوبة تستوجب لكل من قام بصنع وثيقة مكتوبة أو تغيير متعمد للحقيقة بأي وسيلة كانت في كل سند؛ سواء أكان ماديا أو غير مادي؛ من وثيقة معلوماتية أو إلكترونية أو ميكروفيلم أو ميكروفيش، ويكون موضوعه إثبات حق أو واقعة منتجة لآثار قانونية [1].

أما عن المشرع الجزائري فقد انتهج نهج المشرع المصري [2]، إذ أنه لم يقدم تعريفا لجريمة التزوير سواء التقليدية أو الإلكترونية، وإنما اكتفى بالنص في قانون العقوبات على أنواع جرائم التزوير، والتي تتمثل في التزوير في المحررات الرسمية أو العمومية الواردة في المواد (214 إلى 217)، والتزوير في المحررات التجارية أو المصرفية أو العرفية في المادتين (219 و220)، وكذا التزوير في بعض الوثائق الإدارية والشهادات وذلك من خلال المواد (من 222 إلى 229).

من خلال استعراض التعريفات السابقة نصل إلى أن التزوير الإلكتروني هو تغيير للحقيقة عن طريق الغش، كإدخال بيانات غير مطابقة للحقيقة على المحرر الإلكتروني أو تزوير التوقيع الإلكتروني في حد ذاته، مما يؤدي إلى تغيير مضمون المحرر والمعاملة الإلكترونية والذي من شأنه إحداث ضرر للغير.

ثانيا: خصائص التزوير الإلكتروني

إن وقوع جريمة التزوير الإلكتروني في عالم افتراضي لا مادي أضفى عليها بعض الخصائص ميزتها بذلك عن جريمة التزوير التقليدية، إذ لا تتعلق هذه الخصائص بالجريمة فحسب، بل تعدت ذلك لتميّز مرتكب الجريمة، وسنحاول توضيح هذه الخصائص فيما يلي:

---

(1)- للإطلاع على نص المادة كاملا راجع المادة 172 من المجلة الجنائية التونسية على الموقع : المجلة الجزائية (cawtar.org)

(2)- لم يقدم المشرع المصري تعريفا للتزوير وإنما جّرم الصور المختلفة للمساس بالمحررات والتواقيع في الشكل الإلكتروني ومن بينها جريمة التزوير وذلك بموجب قانون التوقيع الإلكتروني المصري رقم (15 لسنة 2004) من خلال المادتين (23 و24) منه.

1- صعوبة الكشف عن جريمة التزوير الإلكتروني:

تعتبر جريمة التزوير الإلكتروني جريمة فنية (معلوماتية) غير ملموسة؛ أي أنها لا تترك أثر مادي على المحرر المزّور، فهي جريمة تقع في بيئة افتراضية يتم فيها نقل المعلومات وتبادلها بالنبضات الإلكترونية. وعليه لا يمكن أن نشاهد آثار التغيير بالإضافة أو الحذف الذي يمكن معاينته في جريمة التزوير التقليدي، ولذا تعتبر جريمة التزوير الإلكتروني في العادة من الجرائم صعبة الكشف [1].

ما يزيد من صعوبة كشف جريمة التزوير الإلكتروني كذلك، هو استخدام المجرم لوسائل الحماية الفنية، كأن يقوم بعملية تشفير البيانات أو استخدام كلمات سر أو دس تعليمات خفية فيها، وكذا قلة خبرة الأجهزة الأمنية وعدم تعاون المجني عليه مع السلطات القائمة بالتحقيق؛ إذ في أغلب الحالات يكون –المجني عليه– عبارة عن مصرف أو مؤسسات مالية أو شركات ضخمة، وخوفا من فقدانه لثقة عملائه وكذا تجنب الإضرار بسمعته يكتفي باتخاذ إجراءات إدارية داخلية دون إبلاغ السلطات المختصة [2].

2- جريمة عابرة للحدود:

لا تعترف الجريمة الإلكترونية بصفة عامة بالحدود الجغرافية فهي كما يُطلق عليها جريمة عابرة للدول، أو عابرة للحدود، إذ غالبا ما يكون الجاني في بلد والمجني عليه في بلد آخر، كما يمكن أن يقع الضرر في بلد ثالث. لذا خلقت هذه الطبيعة التي تتميز بها الجريمة الإلكترونية مشاكل عدّة أهمها تحديد الاختصاص القضائي، تحديد القانون الواجب التطبيق،

---

(1)– وفاء صدراتي، آليات مكافحة جريمة التزوير الإلكتروني، أطروحة لنيل شهادة دكتوراه علوم في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة العربي تبسي، تبسة، 2021/2020، ص 37؛ وأيضا، **إلهام بن خليفة**، الحماية الجنائية للمحررات الإلكترونية من التزوير، أطروحة مقدمة لنيل درجة دكتوراه علوم في العلوم القانونية والإدارية، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2016/2015، ص 65.

(2)– نبيلة هبه هروال، جرائم الانترنت –دراسة مقارنة–، أطروحة مقدمة لنيل شهادة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، 2014، ص 49.

وكذا إشكاليات تتعلق بإجراءات المتابعة القضائية، وغيرها من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام.

3- تفرّد صفة الجاني:

إذا كان المستوى العلمي والمعرفي لا يؤثر في ارتكاب الجرائم التقليدية، فإن الأمر يختلف بالنسبة للجرائم الإلكترونية، فالجاني في العادة في هذه الجرائم ما يكون على قدر عال من العلم ومن أصحاب المعارف والمهارات الفنية في مجال الحاسب الآلي وشبكات الانترنت. وفي الغالب ما يكون من المتخصصين في هذا المجال، وعلى قدر عال من الذكاء المصحوب بالاحترافية في مجال المعلومات [1].

وبالتالي فجرائم التزوير الإلكتروني لا تُتركب عن طريق الخطأ، بل هي جرائم مخطط لها بخبرة أشخاص ذوي مهارة فنية عالية وخبرة وذكاء، وهي ذات طابع ذهني علمي تعتمد على المعلومات والمعارف الفنية التي فرضها التقدم العلمي.

الفرع الثاني
البناء القانوني لجريمة التزوير الإلكتروني

تقوم جريمة التزوير الإلكتروني على ركنيين أساسيين كغيرها من الجرائم، وهما الركن المادي والركن المعنوي، حالها في ذلك حال جريمة التزوير التقليدية. إلا أن قيام جريمة التزوير الإلكتروني في بيئة افتراضية أدى إلى أن يتميز الركن المادي لجريمة التزوير الإلكتروني بخصوصية تجعله مختلفا عن التزوير التقليدي، وكذا جعل من أشكال وطرق التزوير تختلف عن المتعارف عنها في البيئة المادية **(أولا)**.

أما بالنسبة للركن المعنوي فيتخذ صورة القصد الجنائي العام ويضاف إليه قصد خاص **(ثانيا)**.

---

(1)–**ناصر حمودي**، الحماية الجنائية للتجارة الإلكترونية، كلية الحقوق، جامعة الجزائر 1، 2015، ص 45.

أولا: الركن المادي

لقيام الركن المادي في جريمة التزوير الإلكتروني يشترط ضرورة توافر عنصرين رئيسيين، يتمثل العنصر الأول في السلوك المادي للجريمة والذي يتمثل في تغيير الحقيقة في محرر إلكتروني بطرق التزوير المحددة قانونا، في حين يتمثل العنصر الثاني في الضرر اللاحق بالغير، وهو ما نبينه في النقطتين التاليتين.

1- السلوك المادي لجريمة التزوير الإلكتروني:

يتمثل السلوك المادي في جريمة التزوير الإلكتروني في تغيير الحقيقة في المحرر بإحدى الطرق التي حددها القانون تغييرا من شأنه إحداث ضرر بالغير، ويقصد بالحقيقة واقعة معينة لا يختلف عليها الأشخاص، هذا إذا ما تعلقت الحقيقة بمحرر رسمي، أما إذا تعلقت بمحرر عرفي فيقصد بها ما اتفق عليه الطرفان [1].

وتغيير الحقيقة يعني إبدالها بما يخالفها، أو إنشاء حقيقة مخالفة، أو تحريف حقيقة قائمة، وأن يكون من شأن هذا التحريف أن يمس بالمركز القانوني للغير. أما إذا ظلت الحقيقة على حالها دون تغيير، فلا تزوير حتى ولو كان الفاعل معتقدا أن ما أثبته مخالفا للواقع [2].

ويتجسد تغيير الحقيقة في بيانات المحرر الإلكتروني في ثلاث صور أساسية؛ فعل الإدخال والذي يقصد به إضافة معطيات جديدة، فعل المحو والذي يراد به إزالة جزء من البيانات المسجلة على المحرر الإلكتروني، فعل التعديل والذي يقصد به تغيير البيانات الموجودة على المحرر الإلكتروني واستبدالها بأخرى[3]. ويستوي أن يكون هذا التغيير كليا أو جزئيا، كما يمكن تصور هذا التزوير في التوقيع الإلكتروني الممهور به المحرر

---

(1)- هلالي عبد الله، شرح قانون العقوبات البحريني -القسم الخاص-، ط1، منشورات جامعة البحرين، 2007، ص 153، مشار إليه لدى **وفاء صدراتي**، مرجع سابق، ص 60.

(2)- إلهام بن خليفة، مرجع سابق، ص 95.

(3)- عزيزة لرقط، الحماية الجنائية للتوقيع والتصديق الإلكترونيين في التشريع الجزائري، مجلة الاجتهاد للدراسات القانونية والاقتصادية، العدد 11، جانفي ،2017، ص 113.

الإلكتروني، ويمكن أن يظهر هذا التزوير على كيان مادي، سواء كان ورقي أو على دعامة إلكترونية كالشرائط الممغنطة والأقراص الإلكترونية وغيرها من الدعامات المماثلة[1].

يفرق بعض الفقه هنا بين تغيير المعلومات المعالجة آليا، وبين إخراج هذه المعلومات سواء على شكل ورقي أو على دعامة إلكترونية. حيث يرى هذا الفريق أن جريمة التزوير الإلكتروني تنصب على مخرجات الحاسب الآلي سواء كانت ورقية أو على دعامة إلكترونية، أي أن يكون لها كيان مادي يمكن إدراكه، وأن تكون معدة للتداول بين الأفراد، ولو تم تغيير الحقيقة دون طباعة فلا يطلق عليه تزوير[2]. إلا أن هناك من دحض هذا الرأي –وهو ما نوافقه– على أساس أن التزوير لم يقع استقلالا، بل وقع نتيجة التلاعب في المعلومات المخزنة على الحاسوب أولا، وكذا لإمكانية إنجاز المعاملات الإلكترونية والتي تؤثر في المراكز القانونية للأفراد دون الحاجة لإخراجها على دعامة مادية؛ إذ يتم تبادل الوثائق بين الأطراف عن طريق شبكة الانترنت، وهو ما يجعلنا أمام حالة كون المعلومات المزورة معالجة آليا وإخراجها من نطاق المحررات التي ينصب عليها التزوير يؤدي بالضرورة إلى فقدان الثقة في هذا النوع من التعاملات، وهو أمر غير منطقي خصوصا في ظل مقصد التشريعات من إضفاء الحماية على التعاملات الإلكترونية[3].

إن تغيير الحقيقة وحده لا يكفي لقيام الركن المادي في جريمة التزوير بل يجب أن يتم بإحدى الطرق المحصورة التي نص عليها القانون، وعلّة ذلك هو حرص المشرع على حصر الدائرة التي يعتبر تغيير الحقيقة فيها تزويرا معاقب عليه، حتى لا يصير كل كذب مكتوب تزويرا. وقد قسم الفقهاء طرق التزوير المحددة في النصوص القانونية إلى قسمين؛ تزوير مادي وهو أن يقع التزوير على المحرر في حد ذاته، وتزوير معنوي وهو أن يقع على مضمون

---

(1)– بلحسيني حمزة، الحماية الجزائية للمستند الإلكتروني، أطروحة مقدمة لنيل شهادة الدكتوراه في العلوم، تخصص قانون البنوك، كلية الحقوق والعلوم السياسية، جامعة جيلالي اليابس، سيدي بلعباس، 2020/2019، ص 198.

(2)– من أنصار هذا الرأي **نجد أحمد حسام طه تمام**، مرجع سابق، ص 357؛ **عبد الفتا بيومي حجازي**، الحكومة الإلكتروني، مرجع سابق، ص 181.

(3)– عبد الرحمان عبد الله حميد آل علي، جرائم التزوير المعلوماتية، د.د.ن، ط1، د.ب، 2009، ص 81، **مشار إليه لدى براهيمي حنان**، مرجع سابق، ص 205؛ **باهة فاطمة**، مرجع سابق، ص 334؛ **وفاء صدراتي**، مرجع سابق، ص 35.

المحرر دون المساس بمادته. هنا نتساءل عن مدى إمكانية ورود طرق التزوير التقليدي على التزوير الإلكتروني؟ وهل هذه الطرق المذكورة حصرا كافية لمجابهة التزوير في المحررات والتواقيع الإلكترونية؟

أ- مدى تطبيق طرق التزوير المادي على أدلة الإثبات الإلكتروني:

التزوير المادي هو ذلك التزوير الذي يتم بطريقة مادية تترك في المحرر أثر يمكن إدراكه بالحواس أو عن طريق خبرة فنية، حيث يقوم هذا النوع من التزوير في الغالب بعد تدوين المحرر[1]، وقد اتجهت التشريعات إلى تحديد طرقه حصرا [2]. وتتمثل طرق التزوير المادي إما بوضع توقيعات مزورة، وإما بإحداث تغييرات في المحررات، أو الخطوط، أو التوقيعات، أو انتحال شخصية الغير والحلول محلها، أو عن طريق الكتابة في السجلات أو غيرها من المحررات العمومية أو بالتغيير فيها بعد اتمامها وقفلها، وكذا إما بتقليد أو تزييف الكتابة أو التوقيع، أو عن طريق اصطناع اتفاقات أو نصوص أو التزامات أو مخالصات أو بإدراجها في هذه المحررات فيما بعد.

ويمكن تصور تغيير الحقيقة في نطاق المحررات والتواقيع الإلكترونية من خلال طرق التزوير المادية وذلك عن طريق التلاعب في المعطيات بالإضافة والحذف والتعديل، والتقليد والاصطناع، وكذا انتحال شخصية الغير أو الحلول محلها.

ويتم التلاعب بالمحررات الإلكترونية عن طريق إدخال بعض البيانات أو المعلومات إلى المحرر، أو بمحو بعض أو كل البيانات مما يجعلها غير صالحة للاحتجاج بها أو الانتفاع منها، كما يمكن تزوير التواقيع الإلكترونية وذلك عن طريق إدخال توقيع عن طريق الماسح الضوئي ويضاف للمحرر الإلكتروني المزور، فيُنسب هذا المحرر لصاحب التوقيع دون أن

---

(1)- رمزي بن الصديق، تزوير المحررات الإلكترونية بين قابلية الخضوع للقواعد التقليدية وضرورة مراعاة الخصوصية، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد7، العدد 2، السنة 2018، ص 206.

(2)- راجع في هذا نصوص المواد: 214 و216 قانون العقوبات الجزائري؛ المادة 211 وما بعدها من قانون العقوبات المصري؛ الفصل 352 من القانون الجنائي المغربي؛ الفصل 172 من المجلة الجزائية التونسي.

تنصرف إرادته لذلك، ويتم كذلك من خلال سرقة منظومة إنشاء التوقيع الإلكتروني واستخدامها بالنسبة للتوقيع الرقمي، فالتوقيع في هذه الحلة يكون سليما إلا أنه لم يصدر من صاحبه [1].

ب- مدى تطبيق طرق التزوير المعنوي على أدلة الإثبات الإلكتروني:

يتحقق التزوير المعنوي بتغيير الحقيقة أثناء تدوين المحرر ابتداء من قبل القائم على تحريره، أي أن التزوير يقع على مضمون المحرر دون المساس بمادته أو شكله، وعليه فهو لا يترك أثرا يمكن إدراكه بالحواس أو اكتشافه عن طريق الخبرة الفنية [2].

وعموما يمكن رد طرق التزوير المعنوي المحددة أيضا حصرا من قبل القانون إلى طريقتين؛ وهما كتابة اتفاقات خلاف التي دونت أو أُملِيت من قبل الأطراف، وكذا تقرير وقائع كاذبة في صورة وقائع صحيحة أو بالشهادة كذبا بأن وقائع قد اعترف بها أو وقعت في حضوره[3].

وعن إمكانية تطبيق طرق التزوير المعنوي على أدلة الإثبات الإلكتروني فإن الأمر وارد في ظل ما نشهده من اتساع استخدام التكنولوجيا في حياتنا اليومية، فتقريبا كل مخالصاتنا من بيع وشراء تتم بطريقة إلكترونية بواسطة بطاقات الدفع الإلكترونية، فيمكن للموظف المكلف بعملية المخالصة أن يثبت سداد جزء من الثمن في حين أن الثمن سدد كليا، أو أن يُثبت التسوية المالية لمعاملة أحد العملاء دون أن تتم فعلا. كما أن أغلب المؤسسات؛ سواء العامة أو الخاصة؛ تعتمد على تقنية المعلومات في إحصاء عدد عمالها وكذا رواتبهم وكمية الإنتاج والتوزيع وكذا تقدير قيمة الربح والخسارة، ويشرف على تسيير هذه البيانات موظف خبير في مجال الحاسب الآلي، فبإمكان هذا الأخير إدخال بيانات على غير الأمر الذي طلب منه.

---

(1)- صالح شنين، الحماية الجنائية للتجارة الإلكترونية -دراسة مقارنة- رسالة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2012، 2013، ص 60.

(2)- عبد الفتا بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، 2008، ص ص 226، 227.

(3)- راجع في كل من هذا نصوص المواد الآتية: المادة 215 من قانون العقوبات الجزائري؛ المادة 213 من قانون العقوبات المصري؛ الفصل 353 من القانون الجنائي المغربي.

تجدر الإشارة في الأخير إلى أنه لا يمكن حصر طرق التزوير الإلكتروني تشريعيا، كون أن التكنولوجيا الحديثة في تطوّر مستمر مما قد يُسفر عن ظهور طرق وأساليب جديدة للتزوير الإلكتروني. وعليه لا يجب أن يكون النص القانوني المجرّم لفعل التزوير عاما ومطلقا ليتمكن من استيعاب أي طريقة جديدة تفرزها لنا التكنولوجيا في مجال التزوير الإلكتروني.

2- الضرر المترتب عن تغيير الحقيقة:

يعتبر الضرر في جريمة التزوير من العناصر اللازمة لقيام الركن المادي للجريمة، بل حتى أن هناك من الفقه من يذهب إلى اعتباره ركنا مستقلا في جريمة التزوير نظرا لأهميته[1]، لكن سواء كان الضرر عنصر من عناصر الركن المادي أو ركنا مستقلا، فإن جريمة التزوير لا تكتمل إلا ترتب عن تغيير الحقيقة ضررا بالغير. ويُعرف الضرر بأنه كل اخلال أو احتمال الاخلال بمصلحة يحميها القانون نتيجة اعترافه بها، ويستوي في ذلك الضرر الكبير والضئيل، والضرر الفعلي والمحتمل، الأدبي والمالي، الخاص والعام [2].

ويجب لقيام جريمة التزوير في المحررات الإلكترونية توافر نية الإضرار بالغير إلى جانب تغيير الحقيقة المنصب على المحرر سواء حدث الضرر بالفعل أو ممكن حدوثه كشرط للمحررات الإلكترونية العرفية، أما المحررات الإلكترونية الرسمية فالضرر يتحقق بمجرد التزوير لأن مجرد تغيير الحقيقة بأحد الطرق المذكورة سابقا يحقق الضرر[3].

كما قد يكون الضرر الناتج عن تغيير الحقيقة ضررا ماديا أو معنويا؛ فالأول هو الذي يصيب المضرور في ذمته المالية، أما الثاني فهو الذي يصيب الشخص في شرفه أو عرضه أو اعتباره أو كرامته.

---

(1)- محمود نجيب حسني، شرح قانون العقوبات (القسم الخاص)، دار النهضة العربية، مصر، 1987، ص 70.

(2)- فوزية عبد الستار، شرح قانون العقوبات (القسم الخاص)، دار النهضة العربية، مصر، 1988، ص247.

(3)- طه عثمان المغربي، تزوير المستند الإلكتروني، مجلة البحوث القانونية والاقتصادية، العدد 72، يونيو 2020، ص 461.

ثانيا: الركن المعنوي

تُعد جريمة التزوير في المحررات من الجرائم العمدية التي تستلزم لاكتمالها توافر الركن المعنوي للجريمة والمتمثل في القصد الجنائي، غير أنه لا يكف القصد الجنائي العام في جريمة التزوير الإلكتروني والمتمثل في علم الجاني على وجه اليقين بفعل تغيير الحقيقة في المحرر، مع توّجه إرادته لإلحاق ضرر بالغير، بل يتطلب الأمر كذلك توفر قصد جنائي خاص والمتمثل في نية الغش؛ بمعنى أن تتجه نية الجاني وقت ارتكاب الفعل إلى استعمال المحرر الإلكتروني المزوّر فيما زوّر من أجله، وهذا ما سنبينه في النقطتين التاليتين:

1- القصد الجنائي العام:

يقوم القصد الجنائي العام في جريمة التزوير الإلكتروني على عنصري العلم والإرادة مثلها مثل جريمة التزوير التقليدي، فإذا انصرفت إرادة الجاني إلى تغيير الحقيقة في المحرر بإحدى طرق التزوير المادي أو المعنوي المحددة قانونا والتي بيّناها سابقا، مع توقعه احتمال حدوث ضرر مادي أو أدبي نتيجة هذا التغيير، توفر القصد الجنائي العام في حقه.

يرتبط عنصر العلم في جريمة التزوير أن يكون الجاني عالما بأنه يُغير الحقيقة في محرر يحظى بحماية القانون، ويستوي في هذا أن يكون المحرر تقليديا أو إلكترونيا، وهذا العلم مفترض فلا يدفع مسؤوليته عن ذلك بجهله[1].

إضافة إلى عنصر العلم وجب أن تنصرف إرادة الجاني إلى تغيير الحقيقة في المحرر الإلكتروني وإلى تحقق نتيجة؛ وهي اشتمال المحرر على بيانات تخالف الحقيقة مهما كانت الطريقة المستعملة في ذلك[2]، ذلك أننا بيّنا سابقا بأن طرق التزوير الإلكتروني لا يمكن حصرها كما هو الحال عليه في التزوير التقليدي.

---

(1)- براهيمي حنان، تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية، مرجع سابق، ص 225.

(2)- فوزية عبد الستار، مرجع سابق، ص 305.

وعليه وجب توفر القصد الجنائي العام بعنصريه العلم والإرادة حتى يُمكن نسبة التزوير الإلكتروني إلى مرتكبه، إذ يجب أن يكون الفاعل عالما بأن إدخال المعلومات والبيانات إلى مضمون المحرر الإلكتروني أو محوها أو إتلافها أو القيام بأي أعمال أخرى من شأنها تغيير الحقيقة في المحرر الإلكتروني يؤدي إلى قيام القصد الجنائي العام في جريمة التزوير الإلكتروني.

2- القصد الجنائي الخاص:

حتى يكتمل الركن المعنوي في جريمة التزوير وجب أن يتوفر على القصد الجنائي الخاص إلى جانب القصد الجنائي العام، ويتمثل القصد الجنائي الخاص في اتجاه نية الجاني إلى استعمال المحرر المزوّر فيما زوّر من أجله، ويتوافر هذا القصد حتى ولو لم يُستعمل هذا المحرر المزوّر فعلا [1]. ورغم ذلك فإن الأمر لا يزال يثير جدلا فقهيا حول مدى كفاية القصد العام لوقوع جريمة التزوير أم لا بد من توافر القصد الخاص؟

ذهب الفقه الإيطالي إلى أنه يكفي لوقع جريمة التزوير في المحررات الرسمية أن يتوافر القصد الجنائي العام وحده بخلاف جريمة تزوير المحررات العرفية، فإنه وجب توافر القصد الجنائي الخاص إلى جانب العام لقيام جريمة التزوير [2].

في حين ذهب الفقه في فرنسا ومصر إلى إلزامية توافر القصد الجنائي الخاص في جميع أنواع التزوير، واستقر على أن القصد الخاص لقيام الركن المعنوي لجريمة التزوير هو اتجاه نية المُزوِر إلى استعمال المحرر المزور للغرض الذي زُور من أجله[3].

وقد نصت اتفاقية بودابست على ضرورة توافر القصد الجنائي الخاص في جرائم التزوير الإلكتروني من خلال المادة (8) منها والتي تنص على أن التزوير الإلكتروني يشكل: «...

---

(1)- إيهاب فوزي السقا، جريمة التزوير في المحررات الإلكترونية، دار الجامعة الجديدة، مصر، 2008، ص 59؛ **علي عبد القادر القهوجي**، مرجع سابق، ص 152.

(2)- مشار لذلك لدى **إلهام بن خليفة**، مرجع سابق، ص 136؛ **وفاء صدراتي**، مرجع سابق، ص 83.

(3)- إيهاب فوزي السقا، المرجع نفسه، ص 59؛ **إلهام بن خليفة**، المرجع نفسه، ص 136 وما بعدها.

1- إدخال، تغيير، مسح، أو إزالة البيانات الإلكترونية، وكل صورة مساس بسير النظام المعلوماتي بنية الغش، للحصول بدون حق على مصلحة اقتصادية لمرتكب الفعل أو لغيره...»[1]، وبذلك فتحت هذه الاتفاقية الباب أمام مشرعي الدول الأطراف فيها إلى اشتراط نية الغش، أو نية الإضرار بالغير لتقرير المسؤولية عن فعل التزوير.

كما نجد كذلك أن صيغة النص الجنائي الفرنسي في تجريم التزوير كانت واضحة في إقرارها لضرورة توفر القصد الخاص في جريمة التزوير، حيث نص على ضرورة وقوع التزوير بنية الغش وفقا لنص المادة (441-1) من قانون العقوبات الفرنسي، والمشار إليها سالفا.

كما نص المشرع الجزائري على هذا الشرط من خلال المادة (215) من قانون العقوبات الجزائري[2]، والمتمثل في تزييف جوهر المحررات بطريقة الغش؛ أي ضرورة اقتران العلم بنية الغش والمتمثلة في استعمال المحرر المزور.

نصل في الأخير إلى أن جريمة التزوير في المحررات والتواقيع الإلكترونية لا تقل أهمية عن تلك التي تتم في المحررات والتواقيع التقليدية، كون أن أغلب التشريعات قد اعترفت بالحجية القانونية لأدلة الاثبات الإلكتروني ومنحتها نفس القيمة القانونية لأدلة الإثبات التقليدي. إلا أننا نرى أنه لا يمكن تطبيق القواعد العامة لجريمة التزوير التقليدي الواقعة على المحررات التقليدية كما هي على الجريمة التزوير الواقعة على المحررات الإلكترونية، بل إن الأمر يحتاج إلى تدخل تشريعي خاص ينظم جريمة التزوير الإلكتروني بشكل مستقل، لأن توسيع النص العام لا يستقيم بالنظر للطبيعة الخاصة لهذه المحررات، سواء من ناحية اكتشافها وصعوبة اثباتها، واتساع طرق ارتكابها نظرا لما تشهده التقنيات الحديثة من تطور علمي وتكنولوجي، والذي أثر على التطور السريع للنشاط الإجرامي في هذا النوع المستحدث من الجرائم، وكذا من

---

(1)- Article 8: Convention sur la cybercriminalité : **«...b. toute forme d'atteinte au fonctionnement d'un système informatique,**
dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui». https://www.europarl.europa.eu/

(2)- تنص المادة 215 من قانون العقوبات الجزائري على أنه: **«يعاقب بالسجن المؤبد كل قاض أو موظف عمومي أو قائم بوظيفة عمومية قام أثناء تحريره محررات من أعمال وظيفته بتزييف جوهرها أو ظروفها بطريق الغش...»**

ناحية آثارها التي لا تقتصر على فرد أو مؤسسة في دولة واحدة وإنما تتجاوز حدود الإقليم باعتبارها من الجرائم العابرة للدول.

المطلب الثاني
جريمة السرقة المعلوماتية

تعتبر جريمة السرقة من أخطر جرائم الاعتداء على الأموال، هذه الأخيرة التي شملها المشرع الجزائري بحماية جزائية خاصة ضمن قانون العقوبات. واستقر الفقه على تعريف جريمة السرقة بأنها "**اختلاس مال منقول مملوك للغير بطريق الغش بنية تملكه**"[1]. في حين عرفها المشرع الجزائري من خلال نص المادة (350) من قانون العقوبات الجزائري على أنها: «**كل من اختلس شيئا غير مملوك له يعد سارقا**»، والحكم نفسه المقرر في تقنين العقوبات الفرنسي وفقا للمادة (311-1).

وعليه يقوم فعل السرقة وفقا للأحكام التشريعية السابقة إذا ما تم الاعتداء على ملكية الأموال المنقولة المملوكة للغير، ولقد تطور الفكر القانوني في سبيل حماية المال المنقول محل جريمة السرقة على مراحل متعددة، إذ اتجهت الحماية في البداية إلى حماية الحق المالي باعتبار الاختلاس في السرقة ينصب على شيء مادي بنية تملكه، لتظهر فيما بعد أنواع من "الطاقة" لا تتفق مع الملكية المادية ولا هي بالشيء المعنوي "كالفكر والجهد الذهني" وترتب على ذلك البحث في حمايتها، وذلك بتطوير مفهوم المنقول محل السرقة في الملكية التقليدية ليشملها، ومن ثم إضافة نصوص خاصة تجرّم الاعتداء عليها بأنواعها المختلفة[2].

غير أن الثورة المعلوماتية أوجدت لنا مفهوما جديدا للمال وهو "المال المعلوماتي"، والذي إن كان في شق منه مادي يتمثل في الدعامات المثبتة عليها المعلومات بما فيها جهاز الحاسوب وما يرتبط به من ملحقات كأجهزة وأدوات الربط والطباعة، والتي لا تثير أي إشكال في حال تطبيق مفهوم السرقة التقليدي عليها، إلا أنه وفي الشق المقابل والذي يفوق في قيمته

(1)- فوزية عبد الستار، مرجع سابق، ص666.

(2)- كوثر شريط، سرقة المعطيات المعلوماتية، مجلة العلوم القانونية والسياسية، عدد 16، جوان 2017، ص 389.

حاليا الجزء المادي، والذي يغلب عليه الطابع المعنوي والمصطلح بتسميته " بالمعطيات المعلوماتية"[1]، والمتمثل في البيانات والمعلومات المخزنة داخل الجهاز– مثل بيانات المحرر أو التوقيع في الشكل الإلكتروني–، ففي هذه الحالة تثار إشكالية مدى اعتبار هذه المعطيات المعلوماتية محلا لجريمة السرقة؟

ولمعرفة ما إذا كانت المعطيات القانونية محلا لجريمة السرقة، نتطرق في البداية لطبيعة محل جريمة السرقة المعلوماتية **(فرع أول)**، ثم لأركانها **(فرع ثان)**.

---

(1)– عرّف المشرع الجزائري المعطيات المعلوماتية بموجب المادة (2/ج) من القانون رقم (09–04) مؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها: **«ج– معطيات معلوماتية: أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها»**. وفي السياق ذاته، عرفت اتفاقية بودابست المعطيات المعلوماتية بموجب المادة (1/ب) بأنها: **«كل تمثيل للوقائع أو المعلومات أو المفاهيم تحت أي شكل وتكون مهيأة للمعالجة الآلية بما في ذلك برنامج معد من ذات الطبيعة ويجعل الحاسب يؤدي المهمة»**.

المعطيات هي مرادف للبيانات، ويقابلها في اللاتينية كلمة (DATUM) وتعني شيء معطى أو مسلم به، أو شيء ما معروف أو مسلم بصحته كحقيقة أو واقعة وجمعها (DATA) وهي التي تستخدم كلاسيكيا في اللغة الإنجليزية، بينما تستخدم في اللغة الفرنسية كمقابل لها كلمة معطيات (Données). راجع في هذا: **غازي عبد الرحمان هيان الرشيد**، الحماية القانونية من جرائم المعلوماتية (الحاسب والانترنت)، أطروحة لنيل درجة الدكتوراه في القانون، كلية الحقوق، الجامعة الإسلامية، لبنان، 2004، ص 97.

وإن كان بعض الفقهاء يميّز بين المعطيات والمعلومات من الناحية القانونية استنادا إلى التمييز بينهما من الناحية التقنية، فالحقيقة أن المعطيات "البيانات" والمعلومات تستخدم كمترادفات في المجال القانوني لعدم وجود أهمية للتمييز بينهما. فالتمييز بينهما هو من وجهة النظر القانونية مسألة فلسفية أكثر منها ذات أثر قانوني لاسيما في مجال دراستنا، فطالما أن المعلومات هي النتيجة المستخلصة من البيانات أو المعطيات فإن كلاهما يتمتع بالحماية القانونية نفسها، والذي يعنينا في هذه الدراسة هو حماية المعلومات بغض النظر عن فحواها، بما في ذلك النصوص المكتوبة، الرسومات، الخرائط، الصوت والصورة، وغيرها من المعلومات الممثلة في مجموعة من الأرقام، بشرط أن تكون هذه المعلومات في هيئة إلكترونية، لذلك سنستعملهما في هذه الدراسة كمترادفين.

الفرع الأول
محل جريمة السرقة المعلوماتية

من المقرر أن محل جرائم الأموال في التشريعات المختلفة وفقا للقواعد العامة، ينصب على مال منقول مادي للغير، فهل الأمر نفسه بالنسبة للسرقة المعلوماتية التي كل ما ترد عليها عبارة عن معطيات ومعلومات وبيانات متبادلة بالطرق الإلكترونية؟ وبالتالي هل تصلح لأن تكون محلا لجريمة السرقة وفقا للنصوص التقليدية المنظمة لهذه الجريمة؟

في الواقع نجد أن هذه الإشكالية قد أخذت نصيبها من الجدل على المستوى القضائي من خلال تدرج الأحكام القضائية الصادرة في هذا الصدد، والتي كانت مصدرا لأحكام تشريعية لاحقة، كما لم يهمل الفقه دراسة هذه الفكرة بين مؤيد ومعارض، وسنتطرق لكل من الجدل القضائي والفقهي حول اعتبار المعطيات المعلوماتية محلا لجريمة السرقة في النقطتين المواليتين.

أولا: مدى اعتبار المعلومات محلا لجريمة السرقة قضائيا

لم يتعرض المشرع الجزائري إلى تجريم سرقة المعطيات المعلوماتية، ولم نتحصل على أحكام أو قرارات للمحكمة العليا تصدت لها، في حين نجد أن القضاء الفرنسي حاول مواجهتها في العديد من أحكامه وإن كان قد تردد واختلف في اعتبار المعطيات المعلوماتية بمعزل عن الإطار المادي الذي يحتوي عليها محلا لجريمة السرقة، وسنحاول عرض أهم ما جاء به كالآتي:

1- الاتجاه الرافض لفكرة الاعتراف بقابلية المعلومات كمحل لجريمة السرقة:

باستقراء أحكام القضاء الفرنسي الصادرة في هذا الصدد، نجد أن أغلبها قد تبنى موقفا رافضا لاعتبار المنقولات المعنوية كمحل لجريمة السرقة، ففي حكم صدر في (1992/11/25) قضى بأن: «**النقل الذي ينصب على المعلومات بشكل مجرد مهما تكن قيمتها، لا يمكن أن ينطبق بشأنه نص المادة (379) من قانون العقوبات التي تتطلب أن**

ينصب فعل الاختلاس على شيء مادي، أما نقل المعلومات الذي ينجم عن أفعال مثل التصوير أو الطباعة، فإنه لا يمكن أن يؤدي إلى نقل حيازة هذه المعلومات التي تظل على الرغم من ذلك في حيازة صاحبها»[1].

كما استبعدت محكمة النقض الفرنسية في حكم لها صادر سنة (1995) أن تكون المعلومات محلا للسرقة، في قضية تتعلق بقيام موظف من مصلحة الضرائب بتصوير بعض المستندات الخاصة بأحد العملاء، وقام بإرسالها لصحفي لنشرها. فقضت المحكمة بأن جريمة إخفاء الأشياء المتحصلة من جريمة الموجهة إلى الصحفي لا تقوم، لأن السرقة تفترض اختلاسا لشيء مملوك للغير، ونسخ المستند وإعادته لا تتحقق فيه العناصر المكونة لجريمة السرقة، وإنما ما يقع في تلك الحالة هو إفشاء للسر المهني [2].

2- الاتجاه المؤيد لفكرة الاعتراف بقابلية المعلومات كمحل لجريمة السرقة:

لم تستمر أحكام القضاء الفرنسي على حالها، بل لوحظ تغيّر في موقف القضاء من هذا النوع من القضايا، ولعل أبرز أحكامها تتعلق بتجريم أحد المتهمين في قضية "لوجابكس" وهو أحد الذين تم فصلهم من أحد الشركات، حيث قام المتهم بالدخول إلى مقر الشركة بغية تصوير مستندات خاصة بالشركة تثبت مدى استقرار المركز المالي والتجاري للشركة، وبالتالي إثبات الفصل التعسفي الذي مسه، وبهذا كانت الانطلاقة على مستوى الأحكام القضائية على إقرار جريمة السرقة في حالة التصوير الفوتوغرافي للمستندات[3].

وبعد صدور جملة من الأحكام القضائية التي تعترف بقابلية المعلومات بأن تكون محلا لجريمة السرقة، نجد أن أحكام القضاء الفرنسي قد استقرت على موقف صريح من خلال الأحكام التي صدرت في كل من قضايا « Bourquin » ، « Antonioli » و « Bluetouff ».

---

(1)- هذا الحكم مشار إليه لدى: **نائلة عادل محمد فريد قورة**، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، لبنان، 2005، ص 134.

(2)- هذا الحكم مشار إليه لدى: **كوثر شريط**، مرجع سابق، ص397.

(3)- هذا الحكم مشار إليه لدى: **الذهبي خدوجة**، الحماية الجزائية للمعاملات الإلكترونية (دراسة مقارنة)، رسالة مقدمة لنيل شهادة الدكتوراه علوم في الحقوق، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية، أدرار، 2019/2018، ص 17.

حيث تتلخص وقائع القرار الصادر في قضية « Bourquin» سنة (1989)، أن عاملين من عمال مطبعة "بوركان" قاما باستعمال أدوات المطبعة لتصوير (47) أسطوانة داخلها، خلال الوقت اللازم لإعادة الإنتاج تتعلق بقائمة العملاء الأثرياء الذين يتعاملون مع المطبعة، ثم أخذا بعد ذلك (70) أسطوانة أخرى بغرض تصويرها خارج المطبعة، بهدف إنشاء شركة منافسة جديدة فيما بعد، وتوبعا بجرم السرقة لتتم إدانتهم من قبل قضاة الموضوع، لترفض محكمة النقض الطعن المقدم من قبلهما ضد قرار محكمة الاستئناف، على أساس توافر جرم السرقة في حقهما بحيث ميزت بين سرقة ال (70) أسطوانة من جهة، وسرقة المضمون المعلوماتي ل (47) أسطوانة خلال الوقت اللازم لنسخها[1].

هذا الحكم جاء واضح الدلالة على أن المعطيات المعلوماتية تصلح لوحدها أن تكون محلا لجريمة السرقة، وهو ما يعتبر سابقة قضائية تختلف عن جملة الأحكام السابقة التي اكتنفها الغموض في مسألة تجريمها لسرقة المستندات المادية، أو المعلومات المخزنة داخل تلك السندات كما في قضية "لوجابكس".

أما الحكم الثاني فيتعلق بقضية « Antonioli » وهو محاسب بإحدى المؤسسات، كان يحوز بحكم وظيفته مستندات حسابية لاستخدامها في إعداد جداول ورسوم بيانية، فقام بتسليمها إلى شخص آخر لأجل إنشاء مؤسسة منافسة دون علم صاحب العمل، فقضت محكمة الاستئناف بإدانته بجريمة السرقة على أساس أنه اغتصب حيازة هذه المستندات واختلس عن طريق الغش المعطيات الحسابية والتجارية المدونة على المستندات والتي تعتبر أموالا معنوية مملوكة قانونا لرب عمله وأوصلها إلى الغير. وقد رفضت محكمة النقض الفرنسية الطعن بالنقض الذي رفعه المتهم ضد هذا القرار بحيث اعتبرت بأن القرار المطعون فيه قد بين جميع العناصر المكوّنة لجريمة السرقة المادية منها أو المعنوية[2].

---

(1)- أحمد حسام طه تمام، مرجع سابق، ص 457؛ **الذهبي خدوجة**، مرجع سابق، ص 18؛ **كوثر شريط**، مرجع سابق، ص395.

(2)- بلحسيني حمزة، مرجع سابق، ص 236.

وفي قرار صادر سنة (2015) عن محكمة النقض الفرنسية في قضية « Bluetouff »، قام « Olivier Laurelli» المدعو « Bluetouff » وعلى إثر تعطل الشبكة الخارجية الخاصة بالوكالة الوطنية للأمن الصحي والغذائي والبيئة والعمل، تمكن مستخدما متصفح بحث من الدخول إلى هذا النظام المحمي عادة باسم مستخدم وكلمة مرور، وقام بتحميل معطيات محمية على عدة دعائم وبثها إلى الغير، فاتهم بالدخول والبقاء غير المصرح بهما في نظام معالجة آلية للمعطيات وسرقة المعطيات، فبرأته محكمة الدرجة الأولى، لكن على إثر استئناف هذا الحكم من قبل النيابة العامة أدين من قبل محكمة الاستئناف بباريس بجرمي البقاء غير المصرح به وسرقة المعطيات، وهو القرار الذي طعن فيه بالنقض، لترفض محكمة النقض الفرنسية نقضه على أساس أنه ثبت بأن المتهم بقي في نظام المعالجة الآلية للمعطيات بعد اكتشافه بأن هذا الأخير محمي، واختلس معطيات واستعملها دون رضا مالكها[1].

بناء على ما ذكر، نرى بأن الحكم الأخير قد أحدث ثورة فيما يتعلق بسرقة المعلومات بذاتها دون الاستناد إلى الدعامة المادية، فعلى خلاف القرارات السابقة والتي ارتبط فيها فعل اختلاس المعلومات باختلاس الدعامة ولو لوقت قصير كاف لإجراء عملية النسخ، نجد أن قضية "بلوتوف" تم تحميل المعطيات المعلوماتية وبثها إلى الغير دون أن تختلس دعامتها المادية، مما أدى بالبعض[2] إلى القول بأن هذا القرار نزع الصفة المادية عن جريمة السرقة.

ثانيا: مدى اعتبار المعلومات محلا لجريمة السرقة فقهيا

أفرزت مسألة تحديد الطبيعة القانونية للمعلومات بأشكالها المتباينة وصورها المختلفة في البيئة الرقمية، وباعتبارها مجرد إشارات أو نبضات إلكترونية غير مرئية تنساب عبر أجزاء نظام المعالجة الآلية وشبكات الاتصال الدولية بصورة آلية، مواقف فقهية متباينة بين مؤيد ومعارض لفكرة قابلية المعلومات باعتبارها محلا يمكن الاعتداء عليه. وقبل الحديث عن الاتجاهات الفقهية التي تصدّت لهذه الفكرة، يتوجّب لزاما إبراز الشروط اللازمة في نظر الفقه

---

(1)- هذا الحكم مشار إليه لدى: **كوثر شريط**، مرجع سابق، ص 396.

(2)- CLAINCHE Julien, Vol d'information: une qualification juridique incertaine, revue documentaliste , sciences de l'information, 2012 /4 (vol 49), p3. www.cairn.info/revue-documentaliste-sciences-de-l-information-2012-4-page-16.htm

لتوفير الحماية القانونية للمعلومات الإلكترونية، ثم التطرق للاتجاهات الفقهية المؤيدة والمعارضة لاعتبار المعلومات محلا لجريمة السرقة.

1- شروط حماية المعلومات جنائيا

حتى تتمتع المعلومات بالحماية القانونية لا بد أن تتوافر لها مجموعة من الشروط تتمثل فيما يلي:

أ - التجديد والابتكار:

لا تكون المعلومة محل حماية جنائية إلا إذا كانت محددة ومبتكرة:

أ/1- التحديد:

حتى تكون المعلومة -باعتبارها رسالة مخصصة للتبليغ- جديرة بالحماية الجنائية يجب أن تكون محددة، وذلك من خلال حصرها في دائرة خاصة بها وتحديد جوانبها، ذلك أن المعلومة التي تفتقر لصفة التحديد لا يمكن أن تكون معلومة حقيقية، فإذا انعدم التحديد انعدمت المعلومة، لأن الاعتداء يجب أن ينصب على محل محدد، وأن يكون هذا الشيء بدوره محلا لحق محدد[1].

أ/2- الابتكار:

يجب أن تكون المعلومة أيضا مبتكرة، أي غير شائعة يسهل الوصول إليها واستخدامها من قبل الكافة، أما إذا كانت المعلومة عامة ومتاحة للجميع، وغير قابلة للارتباط بشخص محدد أو مجموعة من الأشخاص، فلا تكون معلومة مبتكرة وبالتالي لا تكون محلا للحماية[2].

---

(1)- عائشة مذكور، الحماية الجنائية للعقود الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماجستير في القانون، تخصص قانون العقود، كلية الحقوق والعلوم السياسية، جامعة آكلي محند أولحاج، البويرة، 2018، ص 73.

(2)- خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر، أساليب وثغرات، دار الهدى، الجزائر، 2010، ص16.

ب-السرية والاستئثار:

لا يكفي أن تكون المعلومة جديدة ومبتكرة حتى تكون محل حماية جزائية، بل يجب علاوة على ذلك أن يتوافر لها السرية والاستئثار:

ب/1- السرية:

يشترط أن تكون المعلومة سرية حتى يمكن القول بوقوع تعد عليها ومن ثم الحاجة إلى حمايتها، بخلاف ما إذا كانت المعلومة مكشوفة وكان مجال حركتها غير محدود بمجموعة من الأشخاص. وعليه تكون المعلومة سرية إذا كان المجال الذي تتحرك فيه الرسالة التي تحملها محدد بمجموعة من الأشخاص، فإذا انعدم هذا التحديد كانت المعلومة مكشوفة وقابلة للتداول وغير سرية، ولا يمكن أن تكون محلا للاعتداء وبالتالي محلا للحماية، كالمعلومات المتعلقة بحدث معين أو حقيقة معينة فهي معلومات تفتقد للسرية ولا يمكن أن تكون محلا يعتدى عليه[1].

وتكتسب المعلومة سريتها بالنظر إلى طبيعتها أو بالنظر إلى رغبة صاحبها أو للأمرين معا، كما هو الحال بالنسبة للرقم السري لبطاقة الائتمان، ولا شك أن القيمة الاقتصادية للمعلومة ترتبط بسريتها لأن قيمتها تنخفض كلما زاد عدد العارفين بها، كما ترتبط بمدى سهولة أو صعوبة حصول الغير عليها بوسائله الخاصة، والطابع السري للمعلومة هو الذي يحدد نطاق استعمالها في دائرة محددة ويقلل من استخدامها ويقصرها فقط على دائرة المؤتمنين الذين لهم حق الاستئثار عليها[2].

---

(1)- طعباش أمين، الحماية الجنائية للمعاملات الإلكترونية، بحث مقدم لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام وعلم العقاب، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2013/2012، ص 80.

(2)- سعيداني نعيم، أليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2013/2012، ص25.

وتستمد المعلومة سريتها من كونها موجودة داخل نظام المعالجة الآلية للمعطيات، وأن هذا الأخير مغلق وغير مفتوح للجمهور، ولا يتم الدخول إليه إلا بشروط معينة، كدفع اشتراك، أو الدخول من طرف أشخاص معينين فقط، ومن أهم الجرائم التي تقع على سرية المعطيات جريمة الدخول أو البقاء عن طريق الغش إلى نظام المعالجة الآلية[1].

ب/2- الاستئثار:

حتى تستكمل المعلومة عناصرها القانونية وشروط تمتّعها بالحماية الجزائية يجب أن يتوافر لها شرط الاستئثار، والاستئثار بالمعلومة يعني حيازتها من طرف شخص ما بحيث يصبح هو المتصرف الوحيد فيها وفقا لما تمليه عليه إرادته سواء ببيعها أو إيجارها أو التنازل عنها وغيرها من التصرفات[2].

ج-المعالجة الآلية:

يشترط في المعلومة أيضا حتى تكون جديرة بالحماية -إضافة إلى الشرطين السابقين- أن تكون معالجة آليا، وبعبارة أخرى أن تكون على هيئة إلكترونية، ويقود مثل هذا الأمر إلى حصر نطاق الحماية الجنائية للمعلومات داخل بيئتها الالكترونية فحسب، ليخرج ما دون ذلك من المعطيات التي لم تعالج بعد ولم تدخل إلى نظم معالجة المعطيات، وكذلك المعلومات المعالجة التي انفصلت وسجلت على شيء مادي لأنها أصبحت خارج النظام[3].

2- الاتجاه الفقهي الرافض لاعتبار المعلومات محلا لجريمة السرقة:

يتبنى هذا الاتجاه جانب من الفقه الفرنسي الذي يؤيد فكرة تطبيق المنهج التقليدي الذي يضفي صفة المال على الشي المادي وحده، وبالتالي ينفي أن تكون المعلومات المتداولة

---

(1)- بوخبزة عائشة، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة وهران، 2012-2013، ص10.

(2)- خثير مسعود، مرجع سابق، ص16؛ **طعباش أمين**، مرجع سابق، ص81.

(3)- عبد الفتا بيومي حجازي، التزوير في جرائم الكمبيوتر والانترنت، مرجع سابق ص64؛ **بوبكر رشيدة**، مرجع سابق، ص48.

إلكترونيا محلا لجريمة السرقة مسلما بالطبيعة الذاتية لها[1]، ولقد برّر أنصار هذا الاتجاه رفضهم على أساس أن جريمة السرقة يجب أن ترد على حق الملكية وفعل الاختلاس يكون بالاعتداء على الحقوق المستأثرة للأفراد، والمعلومات في الأصل ملكية عامة لا يمكن نسبتها لأحد[2].

علاوة على ذلك، يأخذ المحل في جريمة السرقة طبيعة مادية، والخاصية المادية للأشياء هي التي تكسبها فرصة الاستغلال والاعتداء وانتقال الحيازة. وعليه فإن الأشياء المعنوية غير المحسوسة بطبيعتها يصعب الاعتراف بإسقاط السلطات المادية عليها كالملكية والحيازة.

ويزيد هذا الاتجاه من تبرير رفضهم قابلية المعلومة للسرقة من خلال افتراض وقوع الاختلاس المكون في انتقال الحيازة من شخص لآخر، ولا يتصور ذلك بنظرهم إلا إذا وقع على الوسيط أو الإطار المادي الذي يتم تخزين المعلومات عليه، والحصول على المعلومة بطريقة غير مشروعة، ودون إذن صاحبها يبرر قيام جريمة التقليد، وهو ما يتطلب تجريمها بنص خاص يجرم فعل النسخ غير المشروع بعيدا عن فكرة الحيازة غير المشروعة [3].

وعليه ووفقا لهذا الاتجاه، تدخل المحررات الإلكترونية وما تحويه من بيانات ومعلومات في نطاق النصوص الخاصة بجريمة السرقة التقليدية إذا ما أفرغت في دعامة مادية كالأسطوانة أو الأشرطة الممغنطة، لاعتبار أن الجريمة تقع على محل مادي يتمثل في هذه الدعامة.

---

(1)- لمزيد من التفصيل حول هذه الآراء الفقهية راجع كل من: **بلحسني حمزة**، مرجع سابق، ص 236 وما يليها؛ **الذهبي خدوجة**، مرجع سابق، ص 21 وما يليها؛ **ناصر حمودي**، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص 148؛ **طعباش أمين**، مرجع سابق، ص 81 وما يليها.

(2)- **نائلة محمد فريد قورة**، مرجع سابق، ص 117؛ **بوبكر رشيدة**، مرجع سابق، ص 61.

(3)- **عمر الفاروق الحسيني**، لمحة عن جرائم السرقة من حيث اتصالها بنظم المعالجة الآلية للمعلومات، ورقة بحثية قدمت في مؤتمر الكمبيوتر والانترنت، جامعة الإمارات (1-3 ماي 2000)، ص 32.

3- الاتجاه الفقهي المؤيد لاعتبار المعلومات محلا لجريمة السرقة:

يرى أنصار هذا الاتجاه أن الأحكام القضائية – التي عرضناها سابقا- قد تبنت فكرة قابلية المعلومات لأن تكون محلا لجريمة السرقة من خلال الاعتراف بإعادة انتاج المعطيات المعلوماتية أو الاعتداء على المحتوى المعلوماتي للمحررات الإلكترونية بشكل سلبي وغير شرعي المكون لجريمة السرقة على أساس أن:

* الاعتراف بفكرة تجريم سرقة المعلومات لا يمثل اعتراضا على مبدأ الشرعية الجنائية بل تأكيدا لها؛ ففعل الاختلاس الواقع على المعلومات إنما يتحدد وفقا لطبيعة الشيء محل السرقة، وهذا ما أكده القضاء الفرنسي، والاستيلاء على المعلومات قد يتحقق بالاطلاع أو النسخ غير المشروع ودون الرجوع إلى إذن صاحبها، وعليه يكون الاعتداء موافقا لطبيعة محل الجريمة [1].

* بعض التشريعات أقرت هذه المسألة من خلال نصوصها القانونية التي عرفت جريمة السرقة، كما هو حال المشرع الجزائري والمصري والفرنسي، حيث أوردوا مصلح " شيء" وهو الأمر الذي يوضح مرونة هذا المصطلح واتساعه ليشمل معنى الأشياء المادية وغير المادية كالمعلومات، وعليه يتضح ضرورة عدم اعتبار محل جريمة السرقة أشياء مادية فحسب.

* كما يضيف أنصار هذا الاتجاه، أن تطبيق النص الخاص بجريمة السرقة على المعلومات مجردة عن الوسيط المادي هو نتيجة حتمية للتطوّر القانوني لفعل السرقة. حيث ترى الأستاذة " Delyssac" أنه إذا استمرت فكرة النظر إلى قيام فعل الاختلاس في جرم السرقة بوجهها التقليدي الذي لا يقع إلا على الأشياء المادية دون غيرها؛ فإن ذلك يمثل قصورا للفكر القانوني وتخلفا عن ركب التطور الذي مس الأفعال الاجرامية بصفة عامة، وبالفعل المتعلق بجريمة السرقة بصفة خاصة، فالقواعد القانونية التقليدية لجريمة السرقة قد وضعت في وقت وظرف لا تقبل فيها إلا الشكل المادي لمحل السرقة[2].

---

(1)- هدى حامد قشقوس، مرجع سابق، ص52؛ **علي عبد القادر القهوجي**، مرجع سابق، ص 30؛ **عمر الفاروق الحسيني**، مرجع سابق، ص35.

(2)- مشار له لدى **الذهبي خدوجة**، مرجع سابق، ص 22؛ **علي عبد القادر القهوجي**، المرجع نفسه، ص 30.

يرى أنصار هذا الاتجاه أيضا أن التطورات السريعة التي حدثت في مجال تكنولوجيا المعلومات والتي مازالت مستمرة حتى الآن، جعلت المعلومات تنتشر بصورة كبيرة في مجال المعاملات الإلكترونية المختلفة مما أدى إلى ارتفاع قيمتها عن الأموال المادية، مما دفع بالفقه الحديث إلى البحث عن معيار آخر غير معيار مادية المال، حيث تم اللجوء إلى معيار القيمة الاقتصادية للشيء، حيث يرى أنصار هذا الاتجاه ومن بينهم الأستاذ(CATALA) و(VIVANT) ضرورة الأخذ بالمفهوم الموسع للمال ليشمل إلى جانب الأشياء المادية تلك الأشياء غير المادية بالنظر إلى قيمتها الاقتصادية، وبالتالي فلا مانع عندهم من إضفاء وصف المال على المعلومات ومعاملتها على أساس ذلك مادام أنها تتمتع بقيمة اقتصادية، بل إنها ذات قيمة اقتصادية عالية، فهي تطرح في السوق للتداول مثلها في ذلك مثل أي سلعة ولها سوق تجاري يخضع لقوانين السوق الاقتصادية[1].

ونحن من جانبنا نؤيد ما ذهب إليه أنصار الاتجاه الثاني، الذي اعتبر المعلومات قيمة من القيم المستحدثة بالنظر إلى قيمتها الاقتصادية، إضافة إلى أن ظروف ووقت وضع النصوص القانونية الخاصة بالسرقة، لم تكن المعلومات آنذاك ذات قيمة على عكس المنقولات المادية. غير أنه وفي ظل التطور التكنولوجي ازدادت قيمة هذه المعلومات؛ بل وفاقت قيمة المنقولات المادية، لذا لا بد من توسيع مفهوم النص القانوني ليشمل حالات لم تكن موجودة سابقا؛ مثلما حصل مع تجريم سرقة التيار الكهربائي والتي تم تطبيق نصوص جريمة السرقة التقليدية عليها، وعليه إمكانية اعتبار المعلومات محلا لجريمة السرقة التقليدية.

---

(1)- مشار له لدى **بوكر رشيدة**، مرجع سابق، ص61؛ **نائلة عادل محمد فريد قورة**، مرجع سابق، ص ص119-120؛ **الذهبي خدوجة**، مرجع سابق، ص ص 22-23؛ **ناصر حمودي**، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص148.

الفرع الثاني
أركان جريمة السرقة المعلوماتية

بالعودة إلى تعريف جريمة السرقة في النصوص القانونية التي تطرقنا إليها سابقا[1]، نجدها تتضمن الإشارة إلى محل جريمة السرقة؛ وهو عبارة عن مال الغير المنقول، ثم الركن المادي؛ والذي يتمثل في فعل الاختلاس أو الأخذ دون الرضا. أما الركن المعنوي فيستخلص من الأحكام العامة، ويتألف من القصد العام، بالإضافة إلى القصد الخاص؛ وهو نية التملك. وسنتطرق بالشرح لكل من هذه الأركان، مع بحث مدى إمكانية تطبيق أحكام جريمة السرقة في صورتها التقليدية على جريمة السرقة المعلوماتية.

أولا: الركن المادي لجريمة السرقة المعلوماتية

أهم ما يميز السلوك المادي في جريمة السرقة، هو فعل الاختلاس، والذي يتمثل في سلب حيازة الشيء المادية من مالكه (أو حائزه) بغير رضائه، وهو ما يفرق جريمة السرقة عن جريمتي النصب وخيانة الأمانة، كون الاختلاس يشكل اعتداء على الملكية وعلى الحيازة في آن واحد، على عكس جريمتي النصب وخيانة الأمانة أين يقع الاعتداء فيهما على الملكية فقط [2].

هذا ويعرف الاختلاس في جريمة السرقة بأنه الاستيلاء على الحيازة الكاملة للشيء بعنصريها المادي والمعنوي بغير رضاء مالكه أو حائزه [3]، وبالتالي يشترط لتحقق فعل الاختلاس في جريمة السرقة ضرورة توافر عنصرين أحدهما موضوعي والثاني معنوي؛ يتمثل العنصر الموضوعي للاختلاس في الاستيلاء على الحيازة على نحو يشكل إخراج الشيء من

---

(1)- **راجع في هذا كل من:** المادة (350) قانون العقوبات الجزائري؛ المادة (311-1) قانون العقوبات الفرنسي؛ المادة (399-1) قانون العقوبات الأردني؛ المادة (311) قانون العقوبات المصري.

(2)- لمزيد من التفاصيل راجع في هذا: **ناصر حمودي**، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص 145.

(3)- للحيازة عنصران، عنصر مادي؛ يشمل مجموع الأفعال أو السلطات والتصرفات التي يباشرها الجاني على الشيء، والثاني معنوي؛ وهو أن تتجه نية الحائز إلى الاستئثار بالشيء وانصراف إرادته إلى مباشرة سلطته عليه بوصفه مالكا له، وباجتماع هذين العنصرين معا تتوفر الحيازة الكاملة للحائز. **أنظر في هذا: ناصر حمودي**، الحماية الجنائية للتجارة الإلكترونية، المرجع والموضع نفسهما.

حيازة المجني عليه وإدخاله في حيازة أخرى، في حين يتمثل العنصر المعنوي للاختلاس في عدم رضاء المالك أو الحائز للشيء عن فعل الاختلاس الذي ارتكبه الجاني [1].

وبما أننا بصدد الحديث عن فعل الاختلاس وعناصره في نطاق المعلوماتية، فإن التساؤل يثار حول مدى انطباق التعريف السابق بعنصريه على المحررات الإلكترونية وما تتضمنه من بيانات ومعلومات؟

إن فعل الاختلاس في مجال المعاملات الإلكترونية يأخذ أساليب خاصة؛ كفعل الالتقاط الذهني للبيانات؛ وهو ما ينشأ عن حفظ وتخزين المعلومات بمجرد البصر أو السمع، أو الالتقاط الهوائي للبيانات المعالجة أو المنقولة؛ وهو ما يتماشى وطبيعة عمل ونظام أجهزة الحاسوب وما يتصل بها من توابع تصدر أثناء تشغيلها بإشعاعات كهرومغناطيسية يمكن التقاطها وترجمتها إلى بيانات مرئية، وكذا عملية نسخ ونقل المعلومات من النظام المعلوماتي؛ وهو ما يترجم فعل الأخذ من خلال اتخاذ فكرة النسخ للمعلومات المخزنة على الدعامات المادية[2].

غير أن فكرة اختلاس المعلومات في حد ذاتها لم تكن محل اتفاق بين الفقهاء، إذ أيّد البعض فكرة الاختلاس في حين أنكر البعض الآخر وقوعه على المعلومات.

ويرى أنصار الاتجاه الأول المؤيد لقابلية اختلاس المعلومات الإلكترونية بالاستناد إلى الحجج التالية أن:

---

(1)- في هذا الصدد يرى الدكتور **عبد الله حسين علي محمود** أن: غالبية التشريعات لم تهتم بوسيلة الاستيلاء على الحيازة أو كيفيتها فكل ما يشترط فيها أن تكون بفعل الجاني، فالاستيلاء على الحيازة يمكن أن يكون فعليا كما لو اتخذ الاستيلاء صورة الأخذ أو الانتزاع أو النقل، كما يمكن أن يكون حكميا كالتقاط الشيء الضائع وحبسه بنية تملكه.

أما بالنسبة للعنصر المعنوي لفعل الاختلاس فيرى أنه إذا أخرج شخص شيئا من حيازة مالكه أو حائزه برضائه فإن جريمة السرقة لا تقوم لانتفاء الركن المعنوي في الاختلاس، لأن المالك أو الحائز في هذا الموضع قد رضي بالتخلي أو التنازل عن حيازة الشيء، وإذا توافر الرضا من جانب مالك الشيء فلا تقوم السرقة حتى ولو كان السارق غير عالم بهذا الرضا، هذا ويشترط في الرضا أن يكون سابقا أو معاصرا لنقل الحيازة. لمزيد من التفصيل راجع: **عبد الله حسين علي محمود**، سرقة المعلومات المخزنة في الحاسب الآلي، ط2، دار النهضة العربية، مصر، 2002، ص 262 وما يليها.

(2)- **عبد الله حسين علي محمود**، المرجع نفسه، ص 261؛ **الذهبي خدوجة**، مرجع سابق، ص 24.

- المعلومات تمثل مالا منقولا قياسا على سرقة الكهرباء والتي تمثلها النبضات الكهربائية من خلال الأسلاك، حيث يمكن تحديد قيمة وكمية المعلومات المختلفة من خلال الشريط أو الأسطوانة، وبالتالي فهي صالحة لأن يرد عليها فعل الاختلاس، وبالتالي صالحة لأن تكون محلا لجريمة السرقة[1].
- يمكن أن يتحقق الاستيلاء على المعلومة عن طريق السمع أو المشاهدة، ومن ثم فإنه يمكن وضع المعلومة في إطار مادي عن طريق تحيزها داخل إطار معين والاستئثار به، ويتحقق ذلك إذا قام الشخص الذي التقط المعلومة بتدوينها أو تسجيلها على دعامة ثم عرضها للبيع، وبذلك تنتقل المعلومة من ذمة مالية إلى ذمة مالية أخرى، وبالتالي لم يعد صاحب المعلومة الشرعي هو الوحيد صاحب الحق في احتكارها [2].
- إن طبيعة المعلومات كأموال معنوية يؤدي لأن يكون فعل الاختلاس من جنس الشيء محل الاختلاس؛ فالأشياء المعنوية يمكن اختلاسها باستخدام نشاط مادي كعملية النسخ أو التصوير الذي يتم عن طريقها انتقال المعلومة من الأصل إلى الصورة، كما قد يتوفر نشاط الاختلاس المعلوماتي الذي يتم بواسطة وسائل النظم المعلوماتية كتعديل المعلومات الموجودة فيها أو مسحها، وذلك من أجل اختلاس الأموال المعنوية أو زيادة العناصر الإيجابية في الذمة المالية للجاني، أو لشخص آخر، ولا يمكن القول بأن الجاني لم يسيطر على هذه الأموال، كونه حقيقة قد أخرج هذه الأموال من ذمة المجني عليه وزاد بها العناصر الإيجابية لذمته المالية، خاصة مع ما أصبحت تشكله المعلومات والبرامج والبيانات من قابلية للانتقال وترتيبها لقيم اقتصادية ومالية كبيرة، وتطرح للتداول في السوق مثلها مثل أي سلعة، لذلك يجب للمعلومات بصفة المال تأسيسا على قيمتها الاقتصادية الكبرى، وبهذا تتحقق وجهة النظر القائلة بأن رفض إضفاء وصف الاختلاس على شيء له قيمة اقتصادية؛ هو بلا جدال رفض

---

(1)- طعباش أمين، مرجع سابق، ص 93.

(2)- رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة مقدمة لنيل شهادة الدكتوراه علوم في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2017،2018، ص 194.

مبني على البعد عن الواقع. ويمكن إضافة الأموال المعلوماتية لمجموعة الأموال التي يحميها القانون الجنائي، وبالتالي تجريم أفعال السرقة التي تتعرض لها[1].

في حين يرى أنصار الاتجاه الثاني الرافض لفكرة وقوع فعل الاختلاس على المعلومات أن:

- عدم توفر صفة المنقول في المعلومة، ذلك أن الاختلاس في مجال المعاملات الإلكترونية لا يتم إلا إذا كانت المعلومات مدونة على دعامات مادية، وإن لم يكن الأمر كذلك فإن الأمر يتعلق بخدمات وليس بأموال[2]، وعليه إذا قام صاحب المعلومة ببثها عبر شبكة معينة وقام شخص آخر باعتراضها بوسيلة أو بأخرى كاستعمال كلمة السر مثلا بطريق الغش فإن الأمر لا يتعلق بجريمة السرقة، ويرجع ذلك لعدم توفر صفة المنقول في المعلومات محل البث، فعلى الرغم من توافر سيطرة صاحب المعلومات محل البث عليها بواسطة استعمال كلمة السر بما يصح القول معه بتوفر الحيازة لهذه المعلومات، فإن السرقة لا تقع، وذلك لانتفاء صفة المنقول، إذ أن اختلاس نسخة من صورة أو برنامج لا يحرم صاحبها منها، ولا ينقل الحيازة إلى يد الجاني مثلما هو مطلوب في جريمة السرقة التقليدية[3].
- وذهب بعض الفقه إلى القول بأن وقوع فعل الاختلاس لا يتم على المعلومة بل على الآلة التي توجد بها المعلومة، فالسرقة لا تقع على الأصل بل على وقت الآلة؛ أي ان فعل الاختلاس وقع على آلة الحاسوب ذاتها، وأن هذا الفعل يتمثل في الاستيلاء عليها ولو لوقت قصير جدا وهو الوقت اللازم لنسخ صور للبرامج أو المعلومات الأصلية من خلالها [4]، فسرقة وقت الحاسوب تعد سرقة عادية قياسا على سرقة السيارة واستعمالها دون إذن صاحبها وكذلك سرقة التيار الكهربائي.

---

(1)- ناصر حمودي، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص 151.

(2)- طعباش أمين، مرجع سابق، ص 96؛ **رابحي عزيزة**، مرجع سابق، ص 192.

(3)- ناصر حمودي، الحماية الجنائية للتجارة الإلكترونية، المرجع نفسه، ص 150.

(4)- طعباش أمين، المرجع نفسه، ص97؛ **رابحي عزيزة**، المرجع نفسه، ص 192 وما يليها.

غير أن هذا الجانب من الفقه قد انتقد على أساس أن المعلومات في الوقت الراهن مثلها مثل أي سلعة، تباع وتشترى وتصلح للتعامل عبر الشبكة، ولا يقدح في هذا أنها ليست منقولا، باعتبار المكالمات الهاتفية والطاقة الكهربائية ليست منقولا أيضا، إلا أن القضاء والفقه وبعض التشريعات –بما فيها المشرع الجزائري– قد استقر على تجريم سرقتها، كونها تدخل في نطاق سرقة المنفعة التي تترتب عليها آثارا مادية [1].

أما القول، إن الاختلاس لا يقع على المعلومة بل على الآلة أو وقتها فهو مناف للصواب؛ كون أن الاعتداء على الآلة من خلال سرقة وقتها يقيم جريمة الدخول أو البقاء غير المشروع داخل النظام المعلوماتي، وبالتالي يخضع لنصوص قانونية خاصة [2].

ثانيا: الركن المعنوي لجريمة السرقة المعلوماتية

تتطلب جريمة السرقة وفقا للقواعد العامة وكذا السرقة المعلوماتية إلى جانب توافر الركن المادي ضرورة توافر الركن المعنوي على غرار باقي الجرائم، وتُعد هذه الجريمة من الجرائم العمدية التي تتطلب القصد الجنائي العام، بالإضافة للقصد الجنائي الخاص.

يقوم القصد العام في جريمة السرقة المعلوماتية على عنصرين شأنه في ذلك شأن القصد العام في ضوء القواعد العامة؛ وهما العلم والإرادة، حيث يتطلب في المقام الأول علم الجاني أن المعلومات المسجلة إلكترونيا؛ سواء المعلومات المخزنة داخل النظام المعلوماتي أو المعلومات المسجلة إلكترونيا والمخزنة على دعامات خارجية مثل الأسطوانات والشرائط الممغنطة ليست ملكا له، وفي المقام الثاني يجب أن تتجه إرادة الجاني إلى الاستيلاء على هذه المعلومات.

ويتمثل القصد الخاص في جريمة السرقة بصفة عامة بتوافر نية تملك الشيء المسروق والظهور عليه بمظهر المالك، وكذلك الحال عليه في جريمة السرقة المعلوماتية فيجب أن تتجه

---

(1)– **ناصر حمودي**، الحماية الجنائية للتجارة الإلكترونية، المرجع نفسه، ص 151.

(2)– لمزيد من التفصيل راجع: **حابس يوسف زيدات**، مدى استيعاب النصوص التقليدية للسرقة الإلكترونية –دراسة مقارنة–، مجلة مركز حكم القانون ومكافحة الفساد، العدد 2، دار جامعة حمد بن خليفة للنشر، ديسمبر 2019، ص 9.
https://doi.org/10.5339/rolacc.2019.9

إرادة الجاني إلى الاستيلاء على المعلومات الإلكترونية بغية الاحتفاظ بها، ويظهر فيها بمظهر المالك [1].

إلا أنه وتماشيا مع ما تم ذكره سابقا، بأن أغلب الاعتداءات في مجال السرقة الإلكترونية تتمثل في فعل اختلاس المعلومات الإلكترونية، مع بقاء هذه الأخيرة لدى المجني عليه، في هذه الحالة نصطدم بفكرة مدى قيام نية الشخص في الاعتداء على المعلومات والبيانات المتعلقة بالمحرر الإلكتروني بغرض التملك، وحرمان المجني عليه منها.

في هذا الصدد، يتجه الفقه الجنائي للاعتراف بوجود وقيام القصد الخاص لجريمة السرقة من خلال النظر إلى الجريمة بطبيعتها؛ حيث تعتبر المعلومات الإلكترونية ذات أهمية مالية واقتصادية كبيرة لأصحابها، ونية الجاني في التملك هنا تظهر من خلال الاعتداء على ملكية حق الاستئثار بتلك المعلومة[2]؛ وعليه لا يلزم حرمان المجني عليه من المعلومة بصفة مطلقة، وإنما مجرد مشاركته حق الاستئثار بها بغير رضائه يعتبر اعتداء على ملكيته.

ونافلة القول بالنسبة لمدى استيعاب النصوص التقليدية للسرقة الإلكترونية، فإنه يمكننا القول في هذا الصدد بإمكانية تطبيق القواعد العامة التي تحكم جريمة السرقة على تلك التي تقع في المجال الإلكتروني، دون أن يكون في ذلك أي إخلال بالمبادئ العامة التي تحكم القانون الجنائي، وهذا على أساس أن:

- تطبيق القواعد العامة الخاصة بجريمة السرقة لا يُعد خروجا على مبدأ المشروعية، إذ أن نص تجريم فعل السرقة في القانون الجزائري جاء موسعا، لاستعمال المشرع الجزائري مصطلح "شيء" والتي يدخل في مدلولها الشيء المادي والمعنوي، فمن باب أولى وحماية للمصلحة العامة توسيع فهم مصطلح "شيء" ليشمل العقاب على اختلاس المعلومات الإلكترونية.

---

(1)- **بلحسني حمزة**، مرجع سابق، ص244؛ **طعباش أمين**، مرجع سابق، ص 100.

(2)- لمزيد من التفصيل راجع في هذا: **حطاب كمال**، الحماية الجزائية للتجارة الإلكترونية، أطروحة دكتوراه في العلوم – تخصص علوم قانونية فرع علوم جنائية–، كلية الحقوق والعلوم السياسية، جامعة الجيلالي اليابس، سيدي بلعباس، 2016/2015، ص ص 139، 140؛ **رابحي عزيزة**، مرجع سابق، ص 196؛ **الذهبي خدوجة**، مرجع سابق، ص 29.

- إن الاحتجاج أيضا بكون المعلومات الإلكترونية لا تعتبر منقولا وبذلك عدم اعتبارها محلا لجريمة السرقة، تعتبر في نظرنا حجة لا يمكن التسليم بها، على اعتبار أن التيار الكهربائي والمكالمات الهاتفية من الأموال المعنوية إلا أنها خاضعة لجريمة السرقة، وعليه يمكننا تطبيق نفس الوضع على سرقة المعلومات الإلكترونية، باعتبار أن كل منها استيلاء على الطاقة الكهربائية والمغناطيسية.

- الاعتراف الفقهي للمعلومات الإلكترونية بصفة المال تأسيسا على قيمتها الاقتصادية والمالية الكبيرة، وإمكانية تداولها في السوق مثلها مثل أي سلعة، مما يلزم إضفاء الحماية الجنائية على هذا المال المعلوماتي، ومن صور هذه الحماية الجنائية تجريم أفعال السرقة التي تتعرض لها هذه المعلومات الإلكترونية.

نصل في الأخير، إلى أنه على الرغم من استيعاب النصوص التقليدية للسرقة الإلكترونية، إلا أنه حبذا لو يتدخل المشرع الجزائري لإيراد نص خاص صريح يجرم فيه سرقة المحررات والمعلومات والبيانات الإلكترونية، نظرا للطبيعة الخاصة لهذه المحررات من جهة، وكذلك لطرق الاعتداء عليها، هذا من جانب. ومن جانب آخر لما لها من أهمية كبيرة في استقرار المعاملات الإلكترونية وازدهارها، إضافة إلى خطورة جريمة السرقة على نظم المعلومات وعلى أمن وسلامة المعاملات الإلكترونية.

المبحث الثاني
الحماية الجزائية لأدلة الإثبات الإلكتروني في إطار الجرائم المستحدثة

أثبت الواقع العملي عدم قصور الجرائم الماسة بالمعاملات الإلكترونية على النمط التقليدي للجرائم، بل تعدتها إلى ظهور سلوكيات إجرامية جديدة لم تألفها مبادئ القانون الجنائي التقليدي؛ ظواهر إجرامية حديثة مستجدة تتمتع بذات خصائص التقنية متجاهلة طرق المواجهة الجنائية التقليدية، أطلق عليها مصطلح الجرائم المعلوماتية أو السيبرانية؛ وقد تمس الغير سواء في شخصه (جرائم الاعتداء على الأشخاص) أو في ماله (جرائم الاعتداء على الأموال).

ومن بين جرائم الاعتداء على الأموال –وهذا ما يهمنا في بحثنا هذا– نجد جرائم المساس بأنظمة المعالجة الآلية للمعطيات التي تعتبر أساس التعاملات الإلكترونية؛ والتي تتعرض من خلالها البيانات والمعلومات للانتهاك، وكذا الجرائم التي تمس بآليات التعامل الإلكتروني كتلك التي قد تمس ببيانات التوقيع الإلكتروني أو التي تقع بمناسبة القيام بأعمال التصديق الإلكتروني.

ونظرا لحداثة وخطورة وتنوع صور الاعتداء والخسائر الناجمة عنها، كان لزاما استحداث نصوص خاصة لمواجهة هذا النوع المستحدث من الجرائم لأجل ضمان أمن وسلامة المعاملات الإلكترونية، وهو ما كرسه المشرع الجزائري من خلال التعديلات التي مست إما الشق العقابي أو الإجرائي لقانون العقوبات، لعل أهمها تعديل قانون العقوبات بموجب القانون (04-15) المؤرخ في (10-11-2004) [1]، حيث أفرد القسم السابع مكرر من قانون العقوبات لهذا النوع من الجرائم تحت عنوان " **المساس بأنظمة المعالجة الآلية للمعطيات**" **(مطلب أول).**

وكذا إصداره للقانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين والذي قرر من خلاله حماية جزائية من كل الأعمال التي قد تهدد سلامة التوقيع الإلكتروني **(مطلب ثان).**

---

(1)- قانون رقم 04-15 مؤرخ في 10 نوفمبر 2004، يعدل ويتمم أمر رقم 66-156 مؤرخ في 08 جوان 1966، يتضمن قانون العقوبات الجزائري، ج . ر. ع 71، صادر بتاريخ 10 نوفمبر 2004.

المطلب الأول

الحماية الجزائية في ظل جرائم المساس بأنظمة المعالجة الآلية للمعطيات

إذا كانت كل من المحررات والتواقيع في الشكل الإلكتروني –أدلة الإثبات الإلكتروني– عبارة عن بيانات ومعلومات إلكترونية يتم تبادلها من خلال نظم المعالجة الآلية للمعطيات، فإن المساس بهذه البيانات والمعلومات ونظم معالجتها يُعد مساسا بالمحررات والتواقيع في الشكل الإلكتروني ذاتها، ويترتب على ذلك أن الحماية الجنائية لهذه الأخيرة ستكون من خلال حماية نظم المعالجة الآلية، وكذا البيانات والمعلومات المخزنة فيها أو المتنقلة عبرها.

ولأجل توفير حماية شاملة فقد جرم المشرع الجزائري كل من الدخول أو البقاء غير المشروع إلى نظام المعالجة الآلية للمعطيات **(فرع أول)**. ولم يكتف بذلك فقط بل ذهب إلى توفير حماية مباشرة للمعلومات، وذلك من خلال تجريمه لكل من التلاعب غير المصرح به بالمعلومات **(فرع ثان)**. وكذا تجريمه للتعامل في معلومات غير مشروعة **(فرع ثالث)**.

الفرع الأول

جريمة الدخول أو البقاء غير المشروع في النظام

تعتبر جريمة الدخول غير المشروع لنظم المعالجة الآلية للمعطيات من الجرائم الشكلية، غير أنه في الغالب ما يرتبط بالدخول ارتكاب جرائم أخرى مادية؛ إذ تعتبر البوابة لارتكاب غالبية الأنشطة غير المشروعة في مجال المعلوماتية، لذلك جرمه المشرع الجزائري من خلال المادة (394 مكرر) من قانون العقوبات الجزائري والتي تقابلها المادة (323–1)[1] من قانون العقوبات الفرنسي والمادة (2) من اتفاقية بودابست[2].

(1)- Art 323-1 de C P F: «**Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni…**». Code pénal français, disponible sur le site : https://www.legifrance.gouv.fr

(2)- Art 2 de C C C**: «Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique ...».**

تنص المادة (394 مكرر) أعلاه على أنه: «**يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.**

تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة.

وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة (6) أشهر إلى سنتين (2) والغرامة من 50.000 دج إلى 150.000 دج».

سنحاول من خلال هذا الفرع التطرق إلى تفاصيل هذه الجريمة، وذلك بالتركيز على ركنها المادي **(أولا)**، مع الإشارة إلى الركن المعنوي لهذه الجريمة **(ثانيا)** والعقوبة المقررة لها **(ثالثا)**، على اعتبار أن الركن الشرعي هو النص الذي ذكرناه سالفا.

أولا: الركن المادي للجريمة

جرم وعاقب المشرع الجزائري بموجب المادة (394 مكرر) من قانون العقوبات الجزائري، فعل الدخول أو البقاء في النظام المعلوماتي أو جزء منه وذلك عن طريق الغش، كما ضاعف العقوبة في حال حذف أو تغيير لمعطيات المنظومة.

باستقراء نص المادة (394 مكرر) يتضح لنا بأن الركن لمادي لهذه الجريمة، يتحقق بإتيان سلوك يتمثل في صورة الدخول لنظم المعالجة الآلية للمعطيات أو البقاء فيها، غير أن بعض الفقه اشترط أن تكون هذه النظم مؤمنة بإجراءات فنية، في حين ترى الأغلبية بعدم ضرورة ذلك [1]. وبالعودة لنص المادة أعلاه، نجد أن المشرع الجزائري لم يشترط ذلك، غير أنه

(1)– اختلفت الآراء في هذه المسألة بين مؤيد ومعارض، حيث يتجه جانب من الفقه إلى التضييق من نطاق الحماية الجزائية لتشمل الأنظمة المعلوماتية التي تم إحاطتها بطرق حماية فنية فقط دون تلك التي تركها أصحابها دون طرق حماية فنية مسبقة؛ على أساس أن القانون لا يحمي إلا الأشخاص الحريصين على أنظمتهم الذين يدركون المخاطر التي تُحيط بأنظمتهم وما تحويه من معلومات هامة وسرية. في حين اتجه رأي آخر من الفقه –وهو الغالب– ودعمته في ذلك بعض أحكام القضاء بأنه لا بد من التوسيع في نطاق الحماية الجزائية لتشمل النوعين من الأنظمة المعلوماتية. لمزيد من التفصيل راجع في هذا: **بطيحي نسيمة**، جريمة الدخول أو البقاء غير المشروع إلى النظام المعلوماتي، مجلة الفقه القانوني والسياسي، المجلد01، العدد

نص على صورتين لهذه الجريمة، الأولى بسيطة؛ تتمثل في مجرد الدخول أو البقاء غير المشروع عن طريق الغش. في حين ان الصورة الثانية مشددة؛ وتتمثل في فعل الدخول أو البقاء غير المشروع، مع تعديل أو حذف او تغيير للمعطيات.

يستشف من صياغة المادة أعلاه، أن الركن المادي لهذه الجريمة يقوم على تحقق فعلي الدخول أو البقاء داخل نظام المعالجة الالية للمعطيات أو جزء منه، ويكفي تحقق أحدهما لقيام هذه الجريمة، وعليه وجب تبيان كل من مدلول الدخول والبقاء غير المشروعين، وكذا صورتا الركن المادي لهذه الجريمة وذلك فيما يلي.

1- مفهوم الدخول إلى النظام والبقاء غير المشروع فيه:

يقوم الركن المادي لجريمة الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات على سلوكيين ماديين، يتمثل الأول في فعل الدخول غير المشروع لنظام المعالجة الآلية للمعطيات، في حين يتمثل الثاني في البقاء غير المشروع فيه أو في جزء منه، لذا وجب علينا تبيان كل من مدلول الدخول والبقاء غير المشروعين، وذلك في النقطتين المواليتين.

أ- مدلول الدخول غير المشروع إلى النظام:

للدخول مدلولان، أحدهما معنوي؛ حيث يُشبه الدخول إلى نظام معالجة البيانات أو النظام المعلوماتي بالدخول إلى ذاكرة الإنسان[1]، والثاني مادي؛ ويتمثل في أن الشخص قد حاول أو دخل فعلا إلى النظام المعلوماتي كله أو جزء منه[2].

01، 2019، ص 77؛ وكذلك **حمودي ناصر**، الحماية الجنائية لنظم المعالجة الالية للمعطيات في التشريع الجزائري، المجلة الأكاديمية للبحث القانوني، المجلد 14، العدد02، 2016، ص 73.

(1)- مامن بسمة، جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري، مجلة الحقوق والعلوم السياسية، المجلد 09، العدد01، سنة 2022، ص 479.

(2)- أحمد حسام طه تمام، مرجع سابق، ص 300؛ **حمودي ناصر**، الحماية الجنائية لنظم المعالجة الآلية للمعطيات في التشريع الجزائري، المرجع نفسه، ص 74.

لم يعرف المشرع الجزائري مصطلح الدخول كما لم يحدد الوسيلة التي يتم بها هذا الفعل، لذا يمكن الدخول إلى النظام المعلوماتي بأية وسيلة كانت، سواء عن طريق كلمة السر الحقيقية، أو عن طريق استخدام برنامج او شفرة خاصة، أو حتى باستخدام الرقم الكودي لشخص آخر، فالمهم أن يكون هذا الدخول مخالفا لإرادة صاحب النظام، كما لم يذكر الأفعال المادية لفعل الدخول أو الطريقة التي يتم بها الدخول إلى النظام. لذلك جرم أي طريقة؛ سواء تم الدخول بطريقة مباشرة أو غير مباشرة؛ فقد يعمد الجاني إلى الدخول مباشرة إلى جهاز الحاسب الآلي للضحية، كما يمكن أن يدخل إليه بطريقة غير مباشرة أي عن بعد بجهاز آخر متصل مع جهاز الضحية بواسطة شبكة الانترنت[1].

ولقيام الركن المادي للجريمة، ليس من الضروري أن يقع الدخول إلى كامل النظام المعلوماتي، بل يكفي أن يتم الدخول إلى جزء منه، وهذا ما أكدته المادة (394 مكرر) أعلاه على أن الدخول يتضمن «...**كل أو جزء من منظومة للمعالجة الآلية للمعطيات...**»، وقد جاء هذا التجريم بالمعنى الواسع، وعليه فإن المحل الذي ينصب عليه سلوك الجاني في جريمة الدخول عن طريق الغش في التشريع الجزائري يشمل النظام في حد ذاته، المعلومات التي يحتوي عليها، شبكات المعلومات وحتى المعلومات المنقولة عبرها. وبالتالي يشمل التجريم كذلك عملية اعتراض نقل المعلومات سواء تم عن طريق الدخول إلى شبكات الاتصالات، أو عن طريق التقاط الإشارات التي يحدثها جهاز إلكتروني من خلال وسائل التقاط إلكترونية؛ ويترتب على ذلك أن تصبح هذه الإشارات محلا ينصب عليه سلوك الجاني في جريمة الدخول عن طريق الغش[2].

ب- مدلول البقاء غير المشروع في النظام:

لم يحدد المشرع الجزائري على غرار المشرع الفرنسي وأغلب التشريعات المقارنة المقصود بفعل البقاء، إلا أن الفقه تصدى لهذه المسألة وخصه بعدة تعريفات من بينها تعريف البقاء

(1)- VERON Michel, droit pénal spécial, 9 édition, Dalloz, Paris, 2002, p 280.

(2)- لمزيد من التفصيل راجع في هذا: **رشيدة بوبكر**، مرجع سابق، ص 163؛ **مذكور عائشة**، مرجع سابق، ص 41.

بأنه: **«التواجد داخل نظام المعالجة الآلية للمعطيات ضد من له الحق في السيطرة على هذا النظام»**[1].

وفي المعنى نفسه؛ عرف البقاء بأنه: **«التواجد من قبل الجاني داخل نظام المعالجة الآلية والتجول بين الملفات والمجلدات والبيانات والمعلومات والانتقال من جزء إلى آخر داخل لنظام وبصفة مستمرة»** [2].

كما عُرف بأنه: **«فعل الاتصال بعد ان توافر للشخص العلم بكونه نظاما ممنوعا عليه الدخول إليه واتجاه ارادته إلى الإبقاء على هذا الاتصال الذي حدث بطريق الخطأ»** [3].

وعليه؛ تتحقق جريمة البقاء في غالب الأحيان بعد دخول تم عن طريق الصدفة أو الخطأ، غير ان الجاني وبعد علمه بكونه نظاما ممنوعا الدخول إليه بدون إذن يقرر البقاء وعدم قطع الاتصال، وبالتالي هي جريمة سلوك إيجابي تتحقق بالترك أو الامتناع؛ فامتناعه عن قطع الاتصال مع النظام هو الذي يحقق السلوك الاجرامي المتطلب لقيام هذه الجريمة.

قد يتحقق فعل البقاء غير المشروع داخل النظام المعلوماتي مستقلا عن فعل الدخول وقد يجتمع معه، ويكون البقاء مستقلا عندما يكون الدخول إلى النظام مشروعا، ومن أمثلة ذلك الدخول إلى النظام بطريق الصدفة أو الخطأ أو السهو، في الوقت الذي كان ينبغي على المتدخل أن يقطع تواجده داخل النظام وينسحب منه على الفور، كما تتحقق الجريمة في الفرض الذي يستمر فيه الجاني داخل النظام بعد مرور المدة المحددة له للبقاء[4].

---

(1)- علي عبد القادر القهوجي، مرجع سابق، ص 133.

(2)- بلال أمين زين الدين، جرائم نظم المعالجة الآلية للبيانات في التشريع المقارن والشريعة الإسلامية، دار الفكر الجامعي، مصر، 2008، ص 282، مشار إليه لدى: **بوبكر رشيدة**، مرجع سابق، ص 154.

(3)- عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت (الأحكام الموضوعية والجوانب الإجرائية)، رسالة لنيل شهادة الدكتوراه في القانون الجنائي، كلية الحقوق، جامعة عين شمس، مصر، 2004، ص 332، مشار إليه لدى: **مذكور عائشة**، مرجع سابق، ص 48.

(4)- علي عبد القادر القهوجي، المرجع نفسه، ص 601؛ **بطحي نسيمة**، مرجع سابق، ص 80.

وقد يجتمع فعل الدخول والبقاء غير المشروع داخل النظام المعلوماتي في الفرض الذي يدخل فيه الجاني إلى النظام بطريقة غير مشروعة ويستمر في البقاء داخل النظام بعد ذلك، وينبغي في هذا الفرض تطبيق أحكام التعدد المادي بين الجريمتين [1].

2- صورتا الركن المادي:

تتخذ جريمة الدخول أو البقاء غير المشروع في النظام المعلوماتي صورتان، إحداهما بسيطة، وهي فعل الدخول أو البقاء غير المشروع، في حين أن الثانية مشددة وعقوبتها ضعف العقوبة المقررة للجريمة في صورتها البسيطة، وسنوضح كل صورة مما ذكرنا فيما يلي.

أ- جريمة الدخول أو البقاء غير المشروع في صورتها البسيطة:

بالعودة لنص المادة (394 مكرر) من قانون العقوبات الجزائري التي تقابلها المادة (323-1) من قانون العقوبات الفرنسي نجد أن المشرع الجزائري -على غرار نظيره الفرنسي- يعاقب على مجرد الدخول أو البقاء غير المشروع، ولا يتطلب حدوث نتيجة مادية ضارة معينة، فمجرد قيام الجاني بالدخول غير المشروع إلى النظام أو البقاء فيه تقوم الجريمة ولو لم يتمكن من الوصول إلى معلومات محددة، وبذلك تكون جريمة الدخول من الجرائم الشكلية التي لا يلزم لقيامها تحقق نتيجة مادية معينة [2].

ب- جريمة الدخول أو البقاء غير المشروع في صورتها المشددة:

تنص المادة (394 مكرر ف 2 و3) من قانون العقوبات الجزائري على أنه: «... **تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة.**

وإذا ترتب على الفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة...».

---

(1)- يقصد بالتعدد المادي أن يأت الجاني عدة أفعال مجرمة مستقلة عن بعضها البعض؛ أي لكل من هذه الأفعال أركانها الخاصة دون أن يكون قد صدر حكم نهائي على المتهم بشأن أي منها، ولتفصيل أكثر انظر المواد 33 و34 من قانون العقوبات الجزائري، وراجع كذلك، **عبد الله أوهايبية**، شرح قانون العقوبات الجزائري، القسم العام، دار موفم للنشر، الجزائر، 2009، ص 398.

(2)- **علي عبد القادر القهوجي**، مرجع سابق، ص 610.

نلاحظ من خلال نص هذه المادة، أن المشرع الجزائري قد شدد العقوبة في جريمة الدخول أو البقاء غير المشروع في صورتين؛ سواء ترتب على هذا الدخول أو البقاء غير المشروع حذف أو تغيير معطيات النظام المعلوماتي؛ أو في حالة تخريب نظام اشتغال المنظومة.

ب/1- حذف أو تغيير معطيات النظام المعلوماتي:

يقصد بحذف المعطيات إزالتها، أي جعلها غير متاحة، بينما يقصد بتغيير المعطيات إحداث تعديلات عليها. ويرى الفقه أنه من الصعب التمييز بين فعلي الحذف والتغيير، ذلك أنه لإجراء التغيير فلا مفر من الحذف [1]، وهي جريمة غير التي وردت بنص المادة (394 مكرر 1) المتعلقة بجريمة التلاعب المعلومات، والتي تعد جريمة مستقلة سنتطرق إلى تبيانها لاحقا.

ب/2- تخريب نظام اشتغال المنظومة:

ينصرف التخريب إلى كل فعل من شأنه أن يتسبب في إرباك نشاط أو عمل النظام المعلوماتي [2]، أي جعله غير قابل للاستعمال وأداء الوظائف التي وضع من أجلها، وهي النتيجة الأخطر جسامة التي يمكن تصور إحداثها بالنظام.

ثانيا: الركن المعنوي للجريمة

تعتبر جريمة الدخول أو البقاء غير المشروع جريمة عمدية؛ أي أن تتجه إرادة الجاني إلى الدخول أو البقاء مع علمه أن ذلك يحضره القانون، ويظهر ذلك جليا من عبارة "**عن طريق الغش**" التي استعملها المشرع الجزائري في المادة (394 مكرر) من قانون العقوبات الجزائري المقابلة لعبارة "**Frauduleusement**" التي استعملها المشرع الفرنسي في المادة (323-1) من قانون العقوبات الفرنسي.

وعليه يستبعد من نطاق التجريم الدخول العرضي إلى النظام، كون الواقع العملي يكشف أن الكثير من عمليات الدخول لنظم المعالجة الآلية للمعطيات والبقاء فيها عمليات روتينية

---

(1)- بطحي نسيمة، مرجع سابق، ص 82.

(2)- مذكور عائشة، مرجع سابق، ص 43؛ **بسمة مامن**، مرجع سابق، ص 483.

تتكرر بشكل كبير في اليوم الواحد، لذا لو لم تكن هذه الجريمة عمدية لوقع الملايين من حسني النية تحت طائلة العقاب.

غير أن الفقه اختلف حول طبيعة القصد الجنائي الذي تتحقق به مسؤولية الجاني، بين من اعتبر أن القصد الجنائي العام يكفي لقيام الركن المعنوي، في حين ذهب آخرون إلى أن الجريمة تقوم على القصد الجنائي الخاص إضافة للقصد العام، ويرجع هذا الاختلاف إلى التباين في تفسير مصطلح "Frauduleusement» المنصوص عليه في المادة (323-1) من قانون العقوبات الفرنسي، والذي يقابله مصطلح "عن طريق الغش" الذي استعمله المشرع الجزائري.

إذ يرى أنصار الرأي الأول، وعلى رأسهم الفقيه (Jean.Devése) أن هذه الجريمة لا تتطلب قصدا جنائيا خاصا، بل يكف لقيامها توفر القصد الجنائي العام، كون عبارة عن طريق الغش هي وصف يندرج ضمن ماديات الجريمة، ذلك أن فعل الدخول إلى النظام المعلوماتي في حد ذاته هو سلوك محايد ولا يدل على عدم المشروعية إلا إذا تم دون حق أي عن طريق الغش[1].

في حين يرى أنصار الرأي الثاني، والذي يتزعمه الفقيه (Raymond Gassin) بضرورة توافر القصد الجنائي الخاص إلى جانب القصد العام، كون أن المشرع قصد استعمال عبارة غشا للدلالة على القصد الجنائي الخاص، ولو كان غرض المشرع الاكتفاء بالقصد العام لاستعمل مصطلح "قصدا" أو "عمدا"[2].

ومن جانبنا، نرى أن المادة (394 مكرر) من قانون العقوبات الجزائري لم تتضمن ما يشير إلى وجوب توفر قصد جنائي خاص، أما عبارة " عن طريق الغش" فهي لا تعني هنا نية الإضرار، وإنما تنصرف دلالتها إلى أن دخول الجاني كان دون ترخيص.

---

(1)- JEAN Devése, atteintes aux systèmes de traitement automatisé de données, Juris Classeur, pénal, article (323-1 à 323-7) ,2, 1997, p9, n°10.

مشار له لدى: **بطحي نسيمة**، مرجع سابق، ص 80.

(2)- RAYMOND Gassin, informatique (fraude informatique), répertoire pénal, Dalloz, octobre1995, p22, n°100.

مشار له لدى: **بطحي نسيمة**، المرجع نفسه، ص 80.

ثالثا: عقوبة الجريمة

عاقب المشرع الجزائري بموجب المادة (394 مكرر) من قانون العقوبات[1]، على جريمة الدخول أو البقاء غير المشروع إلى النظام في صورتها البسيطة بعقوبة الحبس من ثلاثة أشهر إلى سنة، وبغرامة من (50.000) دج إلى (100.000) دج، مما يعني بأن هذه الجريمة جنحة وفقا للقانون الجزائري.

وتضاعف العقوبة في حال إذا ترتب على الدخول أو البقاء غير المشروع حذف أو تغيير لمعطيات المنظومة –الصورة المشددة للجريمة–، لتصبح العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من (100.000) دج إلى (200.000) دج.

أما إذا ترتب على الدخول أو البقاء تخريب نظام اشتغال المنظومة فتكون العقوبة من (6) أشهر إلى سنتين والغرامة من (50.000) دج إلى (150.000) دج، وفقا لما نصت عليه المادة (394 مكرر ف 3) من قانون العقوبات الجزائري.

يعاقب المشرع الجزائري كذلك على مجرد المحاولة أو الشروع في ارتكاب هذه الجريمة بنفس العقوبات المقررة للجنحة ذاتها وفقا لنص المادة (394 مكرر 7) من قانون العقوبات الجزائري، كما يعاقب على الاتفاق الجنائي للإعداد لواحدة أو أكثر من هذه الجرائم بالعقوبة نفسها المقررة للجنحة ذاتها وفقا لنص المادة (394 مكرر 5) من القانون ذاته.

أما فيما يخص العقوبات المطبقة على الشخص المعنوي فتتمثل وفقا لنص المادة (394 مكرر 4) من قانون العقوبات الجزائري في غرامة تعادل (5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.

---

(1)– تنص المادة (394 مكرر) من قانون العقوبات الجزائري على أنه: «**يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.**

تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة.

وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة (6) أشهر إلى سنتين (2) والغرامة من 50.000 دج إلى 150.000 دج».

الفرع الثاني
جريمة التلاعب غير المصرح به بالمعلومات

لم يكتف المشرع الجزائري بالحماية التي أقرها للمعلومات من خلال حمايته لنظام المعالجة الآلية –على اعتبار أن المعلومات جزء من النظام–، بل عمد إلى حمايتها مباشرة عن طريق نصوص خاصة مسايرا في ذلك أغلب التشريعات الجنائية المقارنة التي اقتنعت بأهمية المعلومات في الوقت الحالي، وبضرورة حمايتها من كافة أشكال الاعتداء.

قام المشرع الجزائري بتجريم فعل التلاعب غير المصرح به بالمعلومات التي تتضمنها نظم المعالجة الآلية بموجب نص المادة (394 مكرر 1) من قانون العقوبات الجزائري، والتي تقابلها كل من المادة (323–3) من قانون العقوبات الفرنسي [1]، والمادة (4) من اتفاقية بودابست[2]، والتي تنص على ما يلي: **«يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها».**

تقوم جريمة التلاعب العمدي بالمعلومات أو كما وصفها المشرع الجزائري "بطريق الغش"، أو التلاعب غير المصرح به كما تسمى في الفقه المقارن، على ركنين مادي ومعنوي، إضافة للركن الشرعي المتمثل في نص المادة سالفة الذكر، وعليه سنتطرق لركني هذه الجريمة فيما يلي.

أولا: الركن المادي لجريمة التلاعب غير المصرح به بالمعلومات

يقوم الركن المادي لجريمة التلاعب غير المصرح به بالمعلومات وفقا لنص المادة (394 مكرر 1) من قانون العقوبات الجزائري، على سلوك إجرامي يتخذ صورة الإدخال أو التعديل

(1)- Article 323-3 du C P F: **«Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni…».**

(2)- Article 4 - Atteinte à l'intégrité des données**: «1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques. 2. Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux ».**

أو المحو، وأن يرد هذا السلوك على محل معين وهو المعلومات أو المعطيات، يستهدف تحقيق نتيجة معينة تتمثل في تغيير الحالة التي تكون عليها هذه المعلومات في نظام المعالجة الآلية، ولتوضيح أكثر لما تم ذكره سنتطرق لكل نقطة على حدى.

1- السلوك الإجرامي:

يتجسد السلوك الجرمي لجريمة التلاعب غير المصرح به بالمعلومات بحسب نص المادة (394 مكرر 1) من قانون العقوبات الجزائري، بالإدخال أو التعديل أو المحو، كما لم يشترط هذا النص اجتماع هذه الصور، حيث تكفي أي منها لتوافر الركن المادي لهذه الجريمة.

أ- فعل الإدخال:

يتحقق فعل الإدخال بإضافة معطيات جديدة على الدعامة الخاصة به سواء كانت خالية أم يوجد عليها معطيات من قبل، وهو بحسب البعض تغذية للنظام بالمعلومات أو إضافة خصائص ممغنطة جديدة في الدعامة الموجودة، وتكون هذه المعلومات مغلوطة، غير صحيحة، أو خبيثة كالفيروسات، أو صحيحة لكن غير مصرح بإدخالها، وذلك بقصد التشويش على صحة البيانات القائمة[1].

ويتم فعل الإدخال عن طريق استخدام البرامج الخبيثة بغرض التعديل في البيانات، الأمر الذي يؤثر على صحتها أو نسبتها أو قيمتها، كما أنه يكون بغرض إتلافها أو تشويهها أو تدميرها، وهو أمر سهل القيام به خصوصا في المراحل الأولى لتشغيل النظام؛ أي مرحلة إدخال المعلومات، إذ يتم في هذه المرحلة تغذية النظام بمعلومات مغلوطة أو زائفة لم تكن موجودة فيه من قبل، مما يؤثر سلبا على المعلومات الموجودة فيه من حيث سلامتها وقيمتها.

وبالرجوع للتقرير التفسيري لاتفاقية بودابست نجدها تفسر المادة (4) منها السالفة الذكر على أساس أنها جريمة "غش معلوماتي"، وقد ورد في التفسير أيضا أن فعل الإدخال يتضمن إدخال معلومات غير صحيحة على الحاسوب وكذا التلاعب في البرامج الموجودة فيه، وكل

---

(1)- علي عبد القادر القهوجي، مرجع سابق، ص 144؛ **حمودي ناصر**، الحماية الجنائية لنظم المعالجة الآلية للمعطيات، مرجع سابق، ص 80.

التدخلات في معالجة البيانات، وأضاف التقرير أن العقوبة تطال كل تلاعب تعسفي خلال معالجة البيانات بغرض الحصول دون وجه حق على منفعة اقتصادية له أو للغير [1].

ب- التعديل:

يعرف فعل التعديل بأنه: «**تغيير المعلومات الموجودة داخل النظام واستبدالها بمعلومات أخرى**»[2]، كما عرف بأنه: «**كل تغيير غير مشروع للمعلومات والبرامج يتم عن طريق استخدام إحدى وظائف نظام المعالجة الآلية**» [3]، ويعرف أيضا بأنه: «**تغيير لحالة المعطيات الموجودة دون تغيير الطبيعة الممغنطة لها**»[4].

يُعد تعديل المعلومات والبيانات الإلكترونية بصورة غير مشروعة من أكثر صور الإتلاف شيوعا، فالتعديل وفق هذا المعنى قد يتم عن طريق استبدال المعلومات، كما قد يتم عن طريق التلاعب في البرنامج، وذلك بإمداده بمعطيات مغايرة عن تلك التي صمم البرنامج من أجلها، فكثير من البرامج وبعد اعدادها واختبارها قد تمر ببعض التعديلات لتصويب أخطاء اكتشفت بعد العمل بها، وهو ما يتيح إدخال تغييرات من شأنها مساعدة الجاني على إكمال جريمته وكذلك إخفائها[5].

ث-الإزالة:

يعرف فعل الإزالة أو المحو بأنه: «**إزالة جزء من المعلومات المسجلة على دعامة والموجودة داخل النظام، أو تحطيم تلك الدعامة، أو نقل وتخزين جزء من المعلومات إلى**

---

(1)- راجع في هذا التقرير التفسيري لاتفاقية بودابست، ص 11.
https://rm.coe.int/explanatory-report-budapest-convention-in-arabic

(2)- **علي عبد القادر القهوجي**، مرجع سابق، ص144.

(3)- **عز الدين عثماني**، صور الركن المادي في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، مجلة العلوم القانونية والسياسية، المجلد 09، العدد 03، ديسمبر 2018، ص 621.

(4)-**بوكر رشيدة**، مرجع سابق، ص186.

(5)- **نائلة عادل محمد فريد قورة**، مرجع سابق، ص447.

المنطقة الخاصة بالذاكرة»[1]. كما تعرف الإزالة بأنها: **«اقتطاع خصائص مسجلة على دعامة ممغنطة عن طريق محوها أو طمسها، أي ضغط خصائص أخرى فوقها (خصائص جديدة تطمس الخصائص القديمة)، أو عن طريق تحويل ورص خصائص مزالة في منطقة محفوظة من الذاكرة»**[2].

وعلى إثر ذلك تُعد الإزالة مرحلة لاحقة لعملية إدخال المعطيات، فالإزالة تفترض الوجود السابق لعملية الإدخال، وبناء على ذلك يمكن للمسؤولين عن حفظ البيانات وبصورة مبسطة أن يزيلوا المعلومات التي كلفوا بحفظها داخل نظام المعالجة الآلية، ومن أمثلة ذلك محو البيانات التي يحتويها المحرر الإلكتروني على نحو يتم به إحداث تلف للبيانات الإلكترونية عن طريق تعريض الأسطوانات أو الأقراص الممغنطة المسجل عليها المحرر الإلكتروني لقوى مغناطيسية، أو قطع التيار أثناء معالجة البيانات، أو عن طريق التلاعب في البيانات بتغييرها بحيث تفقد قيمتها وحقيقتها التي كانت عليها[3].

تجدر الإشارة أن الأفعال السابقة (الإدخال، التعديل، الإزالة) كصور للركن المادي في جريمة التلاعب بالمعلومات، وردت على سبيل الحصر لا المثال، حيث لا يقع تحت فعل التجريم أي فعل آخر غيرها، حتى لو تضمن المساس بالمعطيات الموجودة داخل نظام المعالجة الآلية للمعطيات، ومن قبيل ذلك نسخ المعلومات أو نقلها لأن ذلك لا ينطوي لا على إدخال ولا على محو أو تعديل بالمعنى السابق ذكره[4] –وإن كان ذلك لا يعني عدم العقاب عليها إطلاقا، حيث أنها تدخل في نطاق الدخول غير المشروع إلى نظام المعالجة الآلية–، وهو الأمر الذي اعتبره الفقه الفرنسي ثغرة تشريعية يجب على المشرع التدخل من أجل

---

(1)– عبد الفتا بيومي حجازي، جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي، مرجع سابق، ص383؛ **علي عبد القادر القهوجي**، المرجع نفسه، ص144.

(2)– محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي –دراسة مقارنة– دار الجامعة الجديدة، مصر، 2007، ص184، مشار إليه لدى **بوكر رشيدة**، مرجع سابق، ص188.

(3)– بلحسيني حمزة، مرجع سابق، ص 223؛ **نائلة عادل محمد فريد قورة**، المرجع نفسه، ص 194.

(4)– علي عبد القادر القهوجي، المرجع نفسه، ص144.

سدها[1]. وذلك ما حدث بالفعل حيث تدخل المشرع الفرنسي ووسّع من نطاق الأفعال التي يتحقق بها السلوك الإجرامي في هذه الجريمة وذلك بموجب تعديل قانون العقوبات في نوفمبر (2014)[2]، حيث أضاف إلى الأفعال السابقة أربعة أفعال أخرى [3]، على عكس المشرع الجزائري الذي ضيّق من نطاق الأفعال التي يتم بها السلوك الإجرامي في جريمة التلاعب العمدي بالمعلومات، وبالتالي من نطاق الحماية الجنائية المقررة لها.

2- محل النشاط الجرمي:

يتمثل محل جريمة التلاعب العمدي بالمعلومات في تلك "المعلومات" التي تمت معالجتها آليا، أي تلك التي أصبحت مجرد إشارات أو رموز، والتي تكون متضمنة داخل النظام باعتبارها جزء منه، وهو ما يستخلص بوضوح من عبارة "**التي يتضمنها**" التي نصت عليها المادة (394 مكرر 1) من قانون العقوبات الجزائري، وبناء على ذلك فإن الحماية الجنائية في هذه الجريمة تشمل المعلومات المعالجة داخل نظام المعالجة الآلية، أو تلك التي هي في طريقها إلى المعالجة بأن اتخذت خطوة أو أكثر من مراحل معالجتها، أو المعلومات المعالجة التي انفصلت عن النظام ثم أعيد إدخالها فيه. أما المعلومات غير المعالجة والتي لم تدخل إلى النظام، أو دخلت ولم تبدأ مراحل معالجتها بعد، أو عولجت وانفصلت عن النظام (كما لو كانت على

---

(1) - Vol de données : modification de l'article 323-3 du Code pénal français, art disponible sur le site suivant :https://www.alain-bensoussan.com/vol-de-donnees-article-323-3-code-penal/2015/02/24/

(2) - loi n° 2014-1353 du 13 novembre 2014 JORF n°0264 du 15 novembre 2014.

(3)- نص عليها المشرع الفرنسي من بموجب المادة (323-3) من قانون العقوبات، إذ عاقب -بالإضافة لأفعال الإدخال والمحو والتعديل- على أفعال الاستخراج، الاحتجاز، إعادة الإنتاج أو النسخ، النقل، بطريق الغش في البيانات التي يحتويها النظام. Voir l'article 323-3 du code pénal française

كذلك المادة 4 من اتفاقية بودابست للجريمة الإلكترونية، والتي تنص على أنه: «**ينبغي على كل طرف أن يعتمد ما قد يلزم من تدابير تشريعية وتدابير أخرى وفقا لقانونه الداخلي لتجريم الفعل المتعمد وغير القانوني المتمثل في الإضرار بالمعطيات المعلوماتية أو حذفها أو إتلافها أو تغييرها أو محوها**». نلاحظ من خلال المصطلحات التي استعملت في هذا النص – الاضرار، الاتلاف...- أنها تعد أكثر عمومية من أفعال الإدخال أو التعديل أو المحو، وأكثر استيعابا لأفعال المساس بالمعطيات المعلوماتية.

قرص أو شريط ممغنط خارج النظام) فهي خارج نطاق الحماية، وإن كان يجوز حمايتها وفقا لنصوص جنائية خاصة[1].

3- النتيجة الإجرامية:

جريمة التلاعب بالمعلومات تشترط وقوع ضرر فعلي على هذه المعلومات، ألا وهو تغيير حالتها، وذلك من خلال الإزالة أو التعديل أو المحو، وبالتالي هي من الجرائم المادية ذات النتيجة، وليست مجرد جريمة شكلية.

مع الملاحظة أن النتيجة في جريمة التلاعب بالمعطيات تقترب من النتيجة التي يترتب عليها تشديد العقاب في جريمة الدخول أو البقاء في نظام المعالجة الآلية، إلا أن الفرق بينهما هو أن ما يترتب على الدخول أو البقاء من تلاعب يكون دائما بعد دخول غير مشروع أو بقاء غير مشروع، كما أن هذا التلاعب غير مقصود، في حين أن النتيجة في جريمة التلاعب بالمعطيات قد تمت بعد دخول أو بقاء مصرح به[2] وأنها دائما مقصودة.

ثانيا: الركن المعنوي لجريمة التلاعب غير المصرّ به بالمعلومات

تُعد جريمة التلاعب غير المصرح به بالمعلومات جريمة عمدية، يتخذ الركن المعنوي فيها صورة القصد الجنائي بعنصريه العلم والإرادة، فيجب أن تتجه إرادة الجاني إلى فعل الإدخال

---

(1)- في هذا المعنى، أنظر كل من: **علي عبد القادر القهوجي**، مرجع سابق، ص143؛ **عبد الفتا بيومي حجازي**، جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، مرجع سابق، ص377؛ **حمودي ناصر**، الحماية الجنائية للتجارة الالكترونية، مرجع سابق، ص31.

(2)- قضي في فرنسا أنه: لا يشترط في المحو أو الإلغاء المعاقب عليه بالمادة 323-3 أن يرتكب بواسطة شخص ليس له حق الدخول.

« …le seul fait de modifier ou supprimer, en violation de la réglementation en vigueur, des données continues dans un système de traitement automatisé, caractérise le délit prévu à l'article 323-3 C P, sans qu'il soit nécessaire que ces modification ou suppression émanent d'une personne n'ayant pas un droit d'accès au système, ni que leur auteur soit animé de la volonté de nuire ainsi, justifie… ». Cass, crim, 8 décembre, 1999

هذا الحكم مشار إليه لدى: **مذكور عائشة**، مرجع سابق، ص 85.

أو المحو أو التعديل، كما يجب أن يعلم الجاني بأن نشاطه الجرمي يترتب عليه التلاعب بالمعلومات، وأن يعلم أيضا أنه ليس له الحق في القيام بذلك، وأنه يعتدي على صاحب الحق في هذه المعلومات أو من له حق السيطرة عليها[1].

أما فيما يخص القصد الجنائي الخاص، فإن المشرع الجزائري لم يستخدم في المادة (394 مكرر 1) قانون العقوبات الجزائري أي عبارة تدل على تطلبه قصد خاص أو نية خاصة لقيام الجريمة، حيث تقوم بمجرد توافر القصد العام على النحو السالف بيانه. أما لفظ الغش الذي استعمله المشرع الجزائري وحتى الفرنسي فإنه لا يدل –كما سبق القول بالنسبة لجريمتي الدخول والبقاء عن طريق الغش– على هذا المعنى، إنما أراد المشرع من خلاله الإشارة إلى أن هذه الجريمة مقصودة أو عمدية[2]، وهذا ما استقر عليه القضاء الفرنسي في عدة أحكام له، منها النقض الجنائي في (08-12-1999)[3].

الفرع الثالث

جريمة التعامل في معلومات غير مشروعة

وفّر المشرع الجزائري من خلال المادة (394 مكرر 2) من قانون العقوبات حماية جزائية للمعطيات المعلوماتية في حد ذاتها دون أن يشترط أن تكون داخل نظام المعالجة الآلية، أو أن يكون قد تم معالجتها آليا، إذ عاقب بموجب هذه المادة على كل من أفعال التصميم أو البحث أو التجميع أو التوفير أو النشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها إحدى جرائم المساس بأنظمة المعالجة الآلية، وهو نفس المعنى الذي أوردته كل من المادة (323-3/1) من قانون العقوبات الفرنسي[4]، والمادة (6)

---

(1)- بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة لنيل شهادة دكتوراه علوم تخصص – قانون عام–، كلية الحقوق، جامعة الجزائر 01، 2018/2017، ص 177.

(2)- علي عبد القادر القهوجي، مرجع سابق، ص145.

(3) - BENSOUSSAN Alain, Fraude informatique, Les atteintes à un système de traitement automatisé de données, en ligne : http://www.alain-bensoussan.com/pages/2903/

(4)- Article 323-3-1 du C P F: «**Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni...».**

من اتفاقية بودابست[1] تحت عنوان إساءة استخدام الأجهزة، وسنفصل أركان هذه الجريمة فيما يلي.

أولا: الركن المادي لجريمة التعامل غير المشروع في المعلومات

تنص المادة (394 مكرر 2) من قانون العقوبات الجزائري على أنه: «**يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج، كل من يقوم عمدا وعن طريق الغش بما يأتي:**

1- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

2- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم».

بناء على هذا النص، يتضح أن لجريمة التعامل غير المشروع في المعلومات صورتين؛ تتمثل الصورة الأولى في التعامل في معلومات صالحة لارتكاب جريمة، في حين تتمثل الصورة الثانية في التعامل في معلومات محصلة من جريمة، وكلتا الصورتان جريمتان شكليتان تنحصران في مجرد السلوك المجرم، دون تطلب أي نتيجة، وهو ما سنبينه فيما يلي.

1- التعامل في معلومات صالحة لارتكاب جريمة:

يتحقق الركن المادي لجريمة التعامل في معلومات صالحة لارتكاب جريمة بإتيان أحد الأفعال المنصوص عليها في المادة (394 مكرر 2 ف 1) من قانون العقوبات الجزائري،

(1)- Article 6 du CCP: «**1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, lorsqu'elles sont commises intentionnellement et sans droit :**
a. la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition.
i. d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 – 5 ci-dessus ;
ii. d'un mot de passe, d'un code d'accès ou des données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2 – 5… »

والتي تتمثل في كل من تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار بالمعلومات، وسنوضح معنى هذه الأفعال فيما يلي.

أ- التصميم:

هو أول عملية في سلسلة التعامل في المعلومات، ويتمثل في إعداد معلومات صالحة لارتكاب جريمة، وعادة ما يقوم به المختصون في المجال كمصممي البرامج الذين يتمتعون بكفاءة ودراية عالية بالبرمجة [1]، مثاله تصميم برامج لأجل الوصول إلى نظم المعالجة الآلية، أو لأهداف تخريبية كالبرامج الفيروسية، أو إنشاء مواقع لاستعمالها في القرصنة الإلكترونية [2].

ب- البحث:

والبحث المقصود هنا هو البحث في كيفية تصميم هذه المعلومات وإعدادها، وليس مجرد البحث عنها داخل المنظومة المعلوماتية، أي البحث عن المعلومات من أجل تصميمها لأغراض تجريمية، مثل البحث عن الشفرات والبيانات التي تمكن من الاستيلاء على التوقيع الإلكتروني للشخص أو فك شفرات تعاملاته المالية الإلكترونية [3].

ج-التجميع:

ويتمثل في القيام بجمع قدر كبير من المعلومات، والتي يمكن استخدامها لارتكاب جرائم الاعتداء على نظم المعالجة الآلية، ولعل استخدام المشرع الجزائري لهذا المصطلح له ما يبرره،

---

(1)- بوبكر رشيدة، مرجع سابق، ص 55؛ **حمودي ناصر**، الحماية الجنائية لنظم المعالجة الآلية للمعطيات في التشريع الجزائري، مرجع سابق، ص 82.

(2)- وكمثال لذلك، قضت محكمة عنابة، قسم الجنح، في القضية رقم 07357/10، بتاريخ 28 -06 -2010 بتوافر الجريمة في حق الشخص الذي قام بتصميم وإنشاء مواقع شبيهة بالمواقع الرسمية لبعض البنوك، وعند محاولة الزبائن إجراء عمليات مصرفية بحساباتهم البنكية وجدوا أنفسهم في المواقع الخاطئة، فيدخلون رقم حساباتهم وكذا أرقامهم السرية، التي كان يستعملها الجاني فيما بعد لتحويل الأموال أو للشراء عبر الإنترنت، وقد قام بتحويل ما قيمته (1.000.000) دولار أمريكي منذ سنة (2005)، وقد كان أغلب ضحاياه زبائن لدى البنك الكندي "**caisse populaire des jardins**"، لمزيد حول تفاصيل هذه القضية راجع: **بوبكر رشيدة**، المرجع نفسه، ص 50.

(3)- حمودي ناصر، الحماية الجنائية لنظم المعالجة الآلية للمعطيات في التشريع الجزائري، المرجع والموضع نفسه.

فتعدد المعلومات من شأنه أن يزيد من درجة الخطورة التي تشكلها، فما من شك أن هناك فرق بين من يحوز معلومة وبين من يسعى إلى تجميعها، فإذا كان الأول خطير فإن الثاني أخطر [1].

في حين آثر المشرع الفرنسي استعمال مصطلح الحيازة "**Détention**" ومن قبيل ذلك حيازة برنامج يسمح بتجاوز إجراءات الحماية الأمنية[2]، وبهذا فإن الحيازة تندرج ضمن مصطلح التجميع، فالتجميع يقتضي وجود عدد من المعلومات المحازة.

د-التوفير:

يقصد به عرض المعلومات وجعلها في متناول الغير وتحت تصرفه وحيازته، ومن قبيل ذلك كلمة المرور، شفرة الدخول، أو أي بيانات معلوماتية تسمح بالدخول على كل أو جزء من نظام المعالجة الآلية، بل إن القضاء الفرنسي توسع في مدلول التوفير ليشمل الكشف أو الإفشاء العلني للثغرات الأمنية في النظام" **La révélation publique de failles de sécurité**"[3].

والتوفير بهذا المعنى يختلف نطاقه عن التجميع من حيث الأشخاص، فالتجميع لا تتعدى فيه عملية حيازة المعلومات والتصرف فيها من يقوم بالتجميع، بينما في التوفير يتعدد الأشخاص الذين سيحصلون على المعلومات ويتصرفون فيها.

هـ-النشر:

يقصد بالنشر إذاعة المعلومات مهما كانت طبيعتها وتمكين الغير من الاطلاع عليها، اعتمادا على مختلف وسائل النشر المتاحة [4]، ووفقا لما جاءت به المذكرة التفسيرية لاتفاقية بودابست فهو كل نشاط من شأنه نقل البيانات للآخرين [5].

---

(1)- بوبكر رشيدة، المرجع نفسه، ص208.

(2) - **BENSOUSSAN Alain**, fraude informatique- cybercriminalité, art disponible sur le site suivant : https://www.alain-bensoussan.com/cybercriminalite-une-nouvelle-incrimination/2010/03/08/

(3) - Cass crim, 27 octobre 2009 ; cass crim, 22 décembre 2009. Disponibles sur le site suivant : https://www.legifrance.gouv.fr

(4)- مليانى عبد الوهاب، أمن المعلومات في بيئة الأعمال الإلكترونية، رسالة لنيل شهادة الدكتوراه في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، 2017/2016، ص 199.

(5)- راجع في هذا التقرير التفسيري لاتفاقية بودابست، ص 12

https://rm.coe.int/explanatory-report-budapest-convention-in-arabic

يعد النشر بهذا المعنى من أخطر الأفعال التي يمكن أن تنصب على المعلومات غير المشروعة، لأن من شأنه نقل هذه المعلومات لعدد كبير من الأشخاص في وقت قياسي، مما يؤدي إلى احتمالية أكبر في أن تستعمل تلك المعلومات في ارتكاب الجرائم، ولذا أحسن المشرع حين جرم هذا السلوك، مما يؤدي إلى التضييق قدر المستطاع من نطاق الأشخاص الذي يحصلون على المعلومات.

و-الاتجار:

يقصد به تقديم المعلومات للغير بمقابل أيا كان نوع هذا المقابل؛ فيستوي أن يكون عينيا أو نقديا أو مجرد خدمة، عكس التوفير الذي قد يكون بدون مقابل، كما يقصد بالاتجار في مجال المعلومات كافة الأفعال التي تكون بمقابل حتى ولو لم ينص عليها القانون التجاري في إطار الأعمال التجارية المنظمة من خلاله [1].

غير أننا نجد أن المشرع الفرنسي قد استعمل مصطلحا آخرا وهو الاستيراد "**L'importation**"، في حين اكتفت اتفاقية بودابست بالإشارة إلى فعلي البيع والاستيراد " **La vente et l'importation**"، غير أن مصطلح الاتجار يتصور وقوعه بالبيع والشراء والاستيراد، وعليه يمكن القول أن المشرع الجزائري قد وسّع في دائرة تجريم التعامل غير المشروع بالمعلومات التي يمكن أن ترتكب بها الجرائم محل دراستنا.

2- جريمة التعامل في معلومات متحصلة من جريمة:

هي الصورة الثانية في التعامل في معلومات غير مشروعة، نص عليها المشرع الجزائري من خلال المادة (394 مكرر 2 فـ2) من قانون العقوبات الجزائري، وتتمثل في التعامل في معلومات متحصلة من جريمة عن طريق الحيازة، الإفشاء، النشر والاستعمال، وهو ما لم ينظمه لا القانون الفرنسي ولا اتفاقية بودابست، ويهدف المشرع الجزائري من وراء تجريم هذا الفعل التضييق من نطاق الأشخاص الذين يمكن أن يتعاملوا في المعلومات المتحصلة من

(1)- دردور نسيم، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة منتوري، قسنطينة، 2013/2012، ص 44.

جرائم الاعتداء المعلومات للحفاظ على ما تبقى من سريتها. وسنحاول شرح هذه الأفعال فيما يلي.

أ-الحيازة:

الحيازة في نطاق القانون الجنائي هي سيطرة إرادية لشخص على شيء، وهي ليست حقا أو مركزا قانونيا، بل مركزا واقعيا. وحيازة المعلومات المتحصلة من إحدى الجرائم السابقة فعل غير مشروع، وفقا لما ورد بنص المادة (394 مكرر2 ف2) من قانون العقوبات الجزائري، ويمكن تشبيه هذه الجريمة بجريمة حيازة أشياء متحصل عليها من جنحة أو جناية [1].

ويقصد بحيازة المعلومات السيطرة الفعلية والإرادية للحائز، إذ يستطيع الحائز إتلاف المعلومات أو تعديلها أو الانتفاع بها أو استعمالها أو توجيهها، مع توافر الإرادة القائمة على نية التملك والسيطرة على المعلومات، مع العلم بذلك [2].

ب-الإفشاء:

يفترض في هذا الفعل انتقال المعلومات من حيازة الجاني إلى غيره من الأشخاص، ولم يتطلب المشرع الجزائري حدوث نتيجة من وراء ذلك بل جرم الفعل لحد ذاته.

ج-النشر:

فعل النشر هنا هو ذاته الذي سبق شرحه من خلال الفقرة الأولى من هذه المادة، غير أن محل الجريمة يختلف، حيث جرم من خلال هذه الفقرة نشر المعلومات المتحصلة من جريمة.

---

(1)- حمودي ناصر، الحماية الجنائية لنظم المعالجة الآلية للمعطيات في التشريع الجزائري، مرجع سابق، ص 83؛ **مليانى عبد الوهاب**، مرجع سابق، ص 200.

(2)- ملياني عبد الوهاب، المرجع والموضع نفسه؛ **مذكور عائشة**، مرجع سابق، ص 96.

د-الاستعمال:

جرّم المشرع الجزائري استعمال المعلومات المتحصل عليها بطريق غير مشروع، أيا كانت نوعية هذا الاستعمال والغرض منه، رغبة منه في غلق الباب أمام أي استعمال لمعلومات متحصل عليها بطرق مجرمة [1].

ثانيا: الركن المعنوي لجريمة التعامل غير المشروع في المعلومات

جريمة التعامل غير المشروع في المعلومات؛ أيا كانت صورتها؛ هي جريمة عمدية تقوم على القصد الجنائي العام بعنصريه العلم والإرادة، وهو ما يستفاد من عبارة " **عمدا**" أو " **عن طريق الغش**" التي وظفها المشرع الجزائري في المادة (394 مكرر 2)، حيث يجب أن يعلم الجاني بكافة العناصر التي تدخل في تكوين الجريمة، أهمها علمه بأنه يتعامل في معلومات غير مشروعة، وأن هذا التعامل قد يستخدم في ارتكاب جريمة، وأن تتجه إرادته إلى القيام بأحد الأفعال السلوكية المنصوص عليها إما بالفقرة (1 أو 2) من المادة (394 مكرر2) من قانون العقوبات، دون اشتراط انصراف إرادته إلى تحقيق نتيجة معينة على اعتبار أن هذه الجريمة من الجرائم الشكلية.

أما بالنسبة للقصد الجنائي الخاص، فيتعين التمييز بين صورتي الجريمة. بالنسبة للصورة الأولى، فهناك من يرى –ونحن نوافقه الرأي– بضرورة توافر القصد من التعامل بهذه المعلومات في الإعداد والتمهيد لاستعمالها في ارتكاب جريمة من الجرائم الماسة بنظام المعالجة الآلية للمعطيات، ذلك أن هذه المعلومات غير معدّة خصيصا لارتكاب جريمة، لأنه ليس من العدالة في شيء مساءلة الشخص لمجرد تعامله في المعلومات بالصور السابقة، فقد لا يكون غرضه من ذلك ارتكاب جريمة، ذلك أن تلك المعلومات ليست معدة خصيصا لارتكاب جريمة، فهي ذات استخدام مزدوج، فكما يمكن أن تستعمل في أغراض غير مشروعة، يمكن أن تستخدم لأغراض مشروعة كأغراض الحماية من الجرائم مثلا، وهو الأمر الذي انتبهت له اتفاقية بودابست عندما اشترطت صراحة في المادة (6) للعقاب على التعامل في الوسائل الصالحة

(1)– حمودي ناصر، الحماية الجنائية لنظم المعالجة الآلية للمعطيات في التشريع الجزائري، مرجع سابق، ص 83.

لارتكاب جريمة أن يكون هذا التعامل بنية استخدامها لغرض ارتكاب جريمة من الجرائم المشار إليها في المواد من (2) إلى (5).

في حين يختلف الأمر بالنسبة للصورة الثانية من الجريمة–جريمة التعامل في معلومات متحصلة من جريمة– فهذه المعلومات مؤكّد أنها متحصلة من جريمة، وبالتالي فإن هذه الطبيعة الثابتة لها تجعل من توافر القصد العام كافيا لقيامها، والدليل على ذلك العبارة التي استعملها المشرع الجزائري في الفقرة (2) من المادة (394 مكرر2) المتمثلة في "**مهما كان الغرض من استعمالها**"، بمعنى أن الجريمة تقوم مهما كان قصد الجاني الذي ينصرف إليه من خلال التعامل في هذه المعلومات.

ما يمكن قوله في ختام هذا المطلب، أن المشرع الجزائري قد هدف من خلال تعديل قانون العقوبات لسنة (2004) إلى مواجهة الاعتداءات المعلوماتية التي تكون نظم المعالجة الآلية عرضة لها، حيث قام بحماية النظام في حد ذاته من كل صور التخريب والافساد والتعطيل وغيرها. ولم يكتف بذلك بل قام بتوسيع مجال حمايته وذلك بتجريمه الاعتداءات الواقعة على المعطيات في حد ذاتها أيا كان شكلها ونوعها وطبيعتها، مما ينجر عنه حماية أدلة الإثبات الإلكتروني المتمثلة في المحرر والتوقيع في الشكل الإلكتروني على اعتبار أنهما معطيات معلوماتية.

المطلب الثاني
الحماية الجزائية في ظل قانون التوقيع والتصديق الإلكترونيين

نظرا لما للتوقيع الإلكتروني من أهمية بالغة في مجال إثبات المعاملات الإلكترونية، وكذا التعريف بأطراف المعاملة الإلكترونية، عمد المشرع الجزائري إلى سن نصوص قانونية خاصة تجرم صور المساس بالتوقيع والتصديق الإلكترونيين، ذلك من خلال الفصل الثاني من القانون (15–04) المتعلق بالتوقيع والتصديق الإلكترونيين، وبتصفح مواد هذا الفصل يتبين أن المشرع الجزائري لم يدرج تقسيما لها، غير أنه باستقراء هذه المواد أمكننا تقسيم الأحكام الجزائية

الضابطة للاعتداء على التوقيع الإلكتروني إلى نوعين، جرائم تتعلق بتداول البيانات **(فرع أول)**، وجرائم أخرى ماسة بنشاط خدمات التصديق الإلكتروني **(فرع ثان)**.

الفرع الأول
الجرائم الماسة بتداول البيانات

جرم المشرع الجزائري في القانون (15-04) سالف الذكر، كل الاعتداءات الماسة ببيانات التوقيع الإلكتروني وشهادة التصديق الإلكتروني ذلك من خلال تجريمه لانتهاك سرية وخصوصية البيانات المتعلقة بالتوقيع الإلكتروني وشهادة التصديق الإلكتروني **(أولا)**، وكذا تجريمه لإساءة استخدام هذه الشهادة **(ثانيا)**، وتشترك كل هذه الجرائم في كونها جرائم عمدية تتطلب لقيامها الركن المعنوي الذي يقوم على القصد الجنائي العام، ولا تحتاج لقصد جنائي خاص، وسنتطرق لهذه الجرائم تباعا فيما يلي.

أولا: جرائم انتهاك سرية وخصوصية البيانات

عاقب المشرع الجزائري على كل سلوك إجرامي يؤدي إلى كشف معلومات سرية تتعلق ببيانات إنشاء التوقيع الإلكتروني وكذا شهادة التصديق الإلكتروني، ذلك بموجب المواد (68، 70، 71، 73) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين، وسنقوم بتبيان كل جريمة على حدى فيما يلي.

1- جريمة التعامل غير المشروع ببيانات توقيع إلكتروني موصوف:

تنص المادة (68) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين على أنه: «**يعاقب بالحبس من ثلاثة (3) أشهر إلى ثلاث (3) سنوات وبغرامة من مليون دينار (1.000.000 دج) إلى خمسة ملايين دينار جزائري (5.000.000 دج)، أو بإحدى هاتين العقوبتين فقط، كل من يقوم بحيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني موصوف خاصة بالغير**».

يتضح من خلال هذه المادة أنه يتطلب لقيام جريمة التعامل غير المشروع ببيانات توقيع إلكتروني موصوف توافر ركن مادي يتمثل في حيازة، أو افشاء، أو استعمال بيانات إنشاء توقيع إلكتروني موصوف خاص بالغير، كما يتطلب لقيامها كذلك توافر الركن المعنوي، وسنوضح كل من ركني الجريمة فيما يلي.

أ-الركن المادي للجريمة:

يقصد ببيانات إنشاء توقيع إلكتروني وفقا للمادة (2 ف3) من القانون (15-04) أنها: **«بيانات فريدة، مثل الرموز أو مفاتيح التشفير الخاصة، التي يستعملها الموقع لإنشاء التوقيع الإلكتروني»**، وقد بيّنا سابقا من خلال الباب الأول من هذه الأطروحة، أن هذه البيانات تكون سرية لا يجب الاطلاع عليها إلا صاحب التوقيع، ولحماية هذه البيانات من كافة أشكال الاعتداء عليها من قبل الغير، جرم المشرع الجزائري أفعال حيازة أو إفشاء او استعمال هذه البيانات من قبل الغير وفقا للمادة (68) أعلاه.

يتمثل السلوك الاجرامي بالنسبة لفعل الحيازة، عندما يتحصل الجاني على بيانات إنشاء التوقيع الإلكتروني الموصوف الخاصة بالغير بطرق غير مشروعة، ويمكن الاستيلاء على هذه البيانات عن طريق النصب المعلوماتي أو خيانة الأمانة [1].

أما عن فعل الافشاء، فهو وضع هذه البيانات في متناول أي شخص مما يزيد من احتمالية الاعتداء عليها، أو استعمالها في أغراض غير مشروعة، ونظرا لإمكانية وقوع هذا الفعل من طرف مؤدي خدمات التصديق الإلكتروني؛ وذلك بكشف مفاتيح التشفير المودعة لديه؛ ألزمه المشرع الجزائري بإدراج توقيعه على شهادة التصديق الموصوفة التي يمنحها، حتى يمكن تحديد مسؤوليته إذا اقتضى الأمر ذلك [2].

---

(1)- جفالي حسين، الحماية الجنائية لتوقيع المستهلك الإلكتروني في التشريع الجزائري، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد 01، العدد03، 2019، ص 272.

(2)- بوبكر رشيدة، مرجع سابق، ص 208.

أما بالنسبة لفعل الاستعمال، فيتم ذلك عادة بالاستيلاء على منظومة التوقيع الإلكتروني التي تحتوي على بيانات إنشاء التوقيع الإلكتروني الموصوف، سواء عن طريق معرفة الرقم السري، أو القرصنة الإلكترونية، أو غيرها، ليتم فيما بعد التوقيع إلكترونيا باستخدام بينات إنشاء التوقيع الإلكتروني الموصوف دون رضاء صاحبه ودون اشتراط حدوث ضرر لصاحب التوقيع، فالمصلحة المحمية هنا هي ثقة التوقيع الإلكتروني، وليس صاحب التوقيع الإلكتروني في حد ذاته.

ب-الركن المعنوي للجريمة:

تعد جريمة التعامل غير المشروع في بيانات توقيع إلكتروني موصوف خاص بالغير من الجرائم العمدية التي ينبغي لقيامها تحقق القصد الجنائي العام بعنصريه، العلم والإرادة، إذ لا بد أن ينصرف علم الجاني إلى أنه يحوز أو يفشي أو يستعمل بيانات إنشاء توقيع إلكتروني موصوف خاص بالغير، وأن تتجه إرادته إلى إتيان أحد المظاهر السلوكية التي نص عليها المشرع الجزائري في المادة (68) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين، رغم علمه بصفتها غير المشروعة.

ج- العقوبة المقررة لجريمة التعامل غير المشروع في بيانات توقيع إلكتروني موصوف:

أخضع المشرع الجزائري المتعامل في هذه البيانات للعقوبة المقررة في المادة (68) من القانون (15-04) سالف الذكر، والمتمثلة في الحبس من ثلاثة (3) أشهر إلى ثلاث (3) سنوات وبغرامة من مليون دينار (1.000.000دج) إلى خمسة ملايين دينار (5.000.000 دج) أو بإحدى هاتين العقوبتين فقط.

في حين يعاقب الشخص المعنوي طبقا للمادة (75)[1] من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين السالف ذكره بغرامة تعادل خمس (5) مرات الحد الأقصى

(1)- تنص المادة (75) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين على أنه: **«يعاقب الشخص المعنوي الذي ارتكب إحدى الجرائم المنصوص عليها في هذا الفصل بغرامة تعادل خمس (5) مرا الحد الأقصى للغرامة المنصوص عليها بالنسبة للشخص الطبيعي».**

للغرامة المنصوص عليها بالنسبة للشخص الطبيعي، وبالتالي يعاقب في هذه الجريمة بغرامة تقدر بخمسة وعشرين مليون دينار (25.000.000 دج).

يجب التنبيه إلى أنه يوجد نص مماثل لهذا النص تضمنه القانون (15-03) المتعلق بعصرنة قطاع العدالة، حيث تنص المادة (17) منه على أنه: «**يعاقب بالحبس من سنة (1) إلى خمس (5) سنوات وبغرامة تتراو من (100.000دج) إلى (500.000دج) كل شخص يستعمل بطريقة غير قانونية العناصر الشخصية المتصلة بإنشاء توقيع إلكتروني يتعلق بتوقيع شخص آخر**».

ما يميز هذا النص أنه يسري فقط على التوقيع الإلكتروني المرتبط بالمحررات الإلكترونية القضائية الصادرة عن وزارة العدل والجهات القضائية التابعة لها، ونظرا لحساسية هذا القطاع شدد المشرع الجزائري في عقوبة الحبس المقررة، في حين خفض من الغرامة، إلا أنه جمع بين العقوبتين فلا مجال للسلطة التقديرية للقاضي في هذه الحالة في توقيع عقوبة الحبس دون الغرامة أو العكس.

2- جريمة إفشاء بيانات شهادة التصديق الإلكتروني:

تنص المادة (70) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين على أنه: «**يعاقب بالحبس من ثلاثة (3) أشهر إلى سنتين (2) وبغرامة من مائتي ألف دينار (200.000 دج) إلى مليون دينار (1.000.000 دج) أو بإحدى هاتين العقوبتين فقط، كل مؤدي خدمات التصديق الإلكتروني أخل بأحكام المادة 42 من هذا القانون**».

فيما تنص المادة (42) من القانون نفسه على أنه: «**يجب على مؤدي خدمات التصديق الإلكتروني الحفاظ على سرية البيانات والمعلومات المتعلقة بشهادات التصديق الإلكتروني الممنوحة**».

من خلال هذين النصين يتبن أنه بالإضافة إلى شرط توافر الركنين المادي والمعنوي للجريمة، يُشترط توافر صفة الجاني، وهذا ما سنوضحه فيما يلي.

أ- صفة الجاني:

لا تقوم هذه الجريمة إلا إذا توفرت في الجاني صفة مؤدي خدمات التصديق الإلكتروني، وهذا ما يميزها عن جريمة الافشاء المنصوص عليها في المادة (68) من القانون نفسه، والتي يكون الجاني فيها من الغير.

وتكمن علة التجريم هنا في أن الجاني قد أؤتمن على المعلومات والبيانات بسبب وظيفته، فمناط العقاب هنا هو الاخلال بالتزام ناشئ عن المهنة وما يترتب عليها من واجب حفظ السر المهني [1].

ب- الركن المادي للجريمة:

يتمثل السلوك الاجرامي في قيام الجاني بإفشاء أو اعلام الغير بالبيانات أو المعلومات الخاصة بشهادة التصديق الإلكتروني، وتنقسم المعلومات أو البيانات الإلكترونية إلى نوعين؛ معلومات متاحة وهي تلك المنشورة على المواقع الإلكترونية للجمهور، ومعلومات سرية أو غير متاحة ويقتصر العلم بها على أشخاص محددين كالموّقع ومؤدي خدمات التصديق الإلكتروني، وهي المعلومات محل الحماية في هذه الجريمة.

وبالتالي يتحقق الركن المادي لهذه الجريمة إذا قام مؤدي خدمات التصديق الإلكتروني بإفشاء البيانات السرية لشهادة التصديق الإلكتروني دون علم صاحبها وبأي وسيلة كانت، ويستوي في المعلومات التي يتم إفشاؤها أن تكون مكتوبة في أوراق أو مسجلة على دعامة إلكترونية أو أن تكون مخزنة ضمن برنامج معلوماتي أو غير ذلك [2].

---

(1)- عزيزة لرقط، مرجع سابق، ص 120.

(2)- فارس خطابي، الحماية الجزائية للتوقيع الإلكتروني، أطروحة لنيل شهادة دكتوراه علوم شعبة الحقوق، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة 1 الحاج لخضر، 2021/2020، ص 169.

ج-الركن المعنوي للجريمة:

تُعد جريمة إفشاء بيانات شهادة التصديق الإلكتروني من الجرائم العمدية التي يكفي لقيامها توافر القصد الجنائي العام بعنصريه العلم والإرادة، إذ وجب ان يعلم الجاني -مؤدي خدمات التصديق الإلكتروني- أنه يقوم بإفشاء البيانات السرية الخاصة بشهادة التصديق الإلكتروني، وأن تتجه إرادته لإتيان السلوك الاجرامي.

د-العقوبة المقررة لجريمة إفشاء بيانات شهادة التصديق الإلكتروني:

عاقب المشرع الجزائري بموجب المادة (70) من القانون (15-04) مؤدي خدمات التصديق الإلكتروني الذي يخل بأحكام المادة (42) من القانون نفسه، بالحبس من ثلاثة (3) أشهر إلى سنتين (2) وبغرامة من مائتي ألف دينار (200.000 دج) إلى مليون (1.000.000) دينار جزائري أو بإحدى هاتين العقوبتين.

في حين يعاقب الشخص المعنوي طبقا للمادة (75) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين السالف ذكره بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المنصوص عليها بالنسبة للشخص الطبيعي، وبالتالي يعاقب في هذه الجريمة بغرامة تقدر خمسة مليون (5.000.000 دج).

3- جريمة جمع البيانات الشخصية للموقع واستخدامها في غير غرضها:

وهي الجريمة المنصوص والمعاقب عليها بنص المادة (71) من القانون (15-04) سالف الذكر، والتي تنص على أنه: «**يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات، وبغرامة من مائتي ألف دينار (200.000 دج) إلى مليون دينار (1.000.000دج) أو بإحدى هاتين العقوبتين فقط، كل مؤدي خدمات تصديق إلكتروني أخل بأحكام المادة 43 من هذا القانون**».

فيما تنص المادة (43) من القانون نفسه على أنه: «**لا يمكن مؤدي خدمات التصديق الإلكتروني جمع البيانات الشخصية للمعني، إلا بعد موافقته الصريحة.**

ولا يمكن مؤدي خدمات التصديق الإلكتروني أن يجمع إلا البيانات الشخصية الضرورية لمنح وحفظ شهادة التصديق الإلكتروني، ولا يمكن استعمال هذه البيانات لأغراض أخرى».

من خلال نص المادة (43) أعلاه، يتضح أن المشرع الجزائري قد فرض على مؤدي خدمات التصديق الإلكتروني التزامين، يتمثل الالتزام الأول في عدم جمع البيانات الشخصية للموقع إلا بعد موافقته الصريحة، في حين يتمثل الالتزام الثاني في عدم استعمال هذه البيانات بطريقة غير مشروعة، وفي حال ما إذا أخل مؤدي خدمات التصديق الإلكتروني بأحد هذين الالتزامين ترتبت عليه مسؤولية جزائية وفقا لنص المادة (71) من القانون نفسه. وفيما يلي سنبين أركان هذه الجريمة والعقوبة المقررة لها.

أ- الركن المادي للجريمة:

يتمثل الركن المادي لهذه الجريمة في قيام مؤدي خدمات التصديق الإلكتروني بجمع البيانات الشخصية للموقع دون الحصول على موافقته، أو استخدام هذه البيانات في غير الغرض الذي جمعت لأجله، وعليه فالسلوك المادي لهذه الجريمة يتمثل في صورتين:

أ/1-الصورة الأولى:

تتمثل في جمع البيانات الشخصية للمعني دون موافقته، وفي هذه الحالة نتصور قيام مؤدي خدمات التصديق الإلكتروني إما بجمع البيانات الشخصية للمعني دون موافقته، أو جمعها على الرغم من رفض المعني لذلك، والعلة من وراء ضرورة الحصول على موافقة الشخص المعني بجمع البيانات، اعتبارها بيانات شخصية تمس بخصوصية الشخص نفسه، وقد تمتد إلى حياته العائلية[1]، كما تعتبر هذه الجريمة من جرائم السلوك إذ يتكون السلوك الاجرامي فيها من أفعال متعددة يكفي توافر إحداها لقيام الجريمة، كما أن توافرها مجتمعة لا يؤدي إلى تعدد الجرائم.

(1)- عزيزة لرقط، مرجع سابق، ص 122.

أ/2- الصورة الثانية:

تتمثل هذه الصورة في استعمال البيانات الشخصية لأغراض أخرى، إذ أن الهدف الأساسي من وراء جمع البيانات الشخصية للمعني هي منحه شهادة التصديق الإلكتروني، فإذا ما استعملها مؤدي خدمات التصديق الإلكتروني في أغراض أخرى غير مسموح له بها تقوم في حقه جنحة استعمال البيانات الشخصية في غير غرضها، وهي من الجرائم السلوكية التي لا تحتاج إلى تحقق نتيجة معينة بل يكفي السلوك الإجرامي لقيام الركن المادي فيها[1].

ب- الركن المعنوي للجريمة:

تعتبر جريمة جمع البيانات الشخصية للموقّع واستخدامها في غير غرضها من الجرائم العمدية، لا بد من توافر القصد الجنائي العام بعنصريه العلم والإرادة لقيامها، ويتحقق القصد الجنائي العام بعلم الجاني -مؤدي خدمات التصديق الإلكتروني- أنه لا يمكنه جمع البيانات الشخصية للمعني دون موافقته، وأن تتجه إرادته إلى إتيان هذا الفعل على الرغم من علمه بأنه ممنوع، هذا بالنسبة للصورة الأولى.

أما بالنسبة للصورة الثانية، فيجب أن يعلم مؤدي خدمات التصديق الإلكتروني أنه يُمنع عليه استخدام البيانات التي جمعها -سواء بطريقة مشروعة أو غير مشروعة- في غير الغرض المخصصة لأجله وهو منح شهادة التصديق الإلكتروني، وإضافة لعلمه بذلك يجب أن تتجه إرادته إلى القيام بهذا السلوك على الرغم من حظره.

أما بالنسبة للقصد الجنائي الخاص والمتمثل في نية الاضرار بصاحب البيانات، فلا يُشترط توافره لقيام هذه الجريمة باعتبارها من جرائم السلوك، فسواء تحقق الضرر أو لم يتحقق يتم متابعة الجاني على هذه الجريمة.

---

(1)- فارس خطابي، مرجع سابق، ص 176.

د- العقوبة المقررة لجريمة جمع البيانات الشخصية للموقع واستخدامها في غير غرضها:

تعاقب المادة (71)[1] من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين، على جمع البيانات الشخصية للموقع واستعمالها في غير الغرض الممنوحة لأجله بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من مائتي ألف دينار (200.000 دج) إلى مليون دينار (1.000.000 دج)، أو بإحدى هاتين العقوبتين فقط.

وتضاعف الغرامة المذكورة أعلاه خمس مرات (5) الحد الأقصى إذا كان مرتكبها شخص معنوي، وفقا لنص المادة (75) من قانون التوقيع والتصديق الإلكترونيين، وعليه تقدر الغرامة المخصصة لهذه الجريمة بالنسبة للشخص المعنوي بخمسة مليون دينار (5.000.000دج).

4- جريمة كشف معلومات سرية أثناء التدقيق:

تنص المادة (73) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين على أنه: «**يعاقب بالحبس من ثلاثة (3) أشهر إلى سنتين (2) وبغرامة من عشرين ألف دينار (20.000 دج) إلى مائتي ألف دينار (200.000 دج) أو بإحدى هاتين العقوبتين فقط، كل شخص مكلف بالتدقيق يقوم بكشف معلومات سرية اطلع عليها أثناء قيامه بالتدقيق**».

كما نص المشرع الجزائري أيضا من خلال الأمر رقم (21-09) المتعلق بحماية المعلومات والوثائق الإدارية[2]، وبموجب المادة (28) على أنه: «**يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 60.000 دج إلى 300.000 دج أو بإحدى هاتين**

---

(1)- تنص المادة (71) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين على أنه: «**يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات، وبغرامة من مائتي ألف دينار (200.000 دج) إلى مليون دينار (1.000.000دج) أو بإحدى هاتين العقوبتين فقط، كل مؤدي خدمات تصديق إلكتروني أخل بأحكام المادة 43 من هذا القانون**».

(2)- أمر رقم (21-09) مؤرخ في 27 شوال عام 1442 الموافق 8 يونيو سنة 2021، يتعلق بحماية المعلومات والوثائق الإدارية، ج.ر.ع 45، صادر بتاريخ 9 يونيو 2021.

العقوبتين، الموظف العمومي الذي ينشر أو يفشي أو يطلع الغير أو يسمح له بأخذ صور من المعلومات أو الوثائق المصنفة "توزيع محدود"[1]

وتكون العقوبة بالحبس من سنة (1) إلى خمس (5) سنوات وبغرامة من 100.000 دج إلى 500.000 دج إذا أدى ذلك إلى المساس بالاعتبار الواجب للسلطات المعنية».

في حين تنص المادة (29) من الأمر نفسه، على أنه: «**دون الإخلال بالعقوبات الأشد المنصوص عليها في التشريع الساري المفعول، يعاقب بالحبس من سنتين (2) إلى خمس (5) سنوات وبغرامة من 200.000 دج إلى 500.000 دج، الموظف العمومي الذي يفشي أو ينشر معلومة أو وثيقة مصنفة "واجب الكتمان" إلى علم الجمهور أو إلى علم شخص لا صفة له في الاطلاع عليها أو يسمح له بأخذ صور منها أو يترك الغير يقوم بذلك.**

وتكون العقوبة الحبس من خمس (5) سنوات إلى عشر (10) سنوات والغرامة من 500.000 دج إلى 1.000.000 دج، إذا كانت الوثائق مصنفة "سري جدا" أو "سري"».

تضح من خلال المواد أعلاه، أنه بالإضافة إلى شرط توافر الركنين المادي والمعنوي للجريمة، يُشترط توافر صفة في الجاني حددها النص، وهذا ما سنوضحه فيما يلي.

---

(1)- تنص المادة (3) من الأمر (21-09) المتعلق بحماية المعلومات والوثائق الإدارية، على أنه: «**يقصد في مفهوم هذا الأمر، بما يأتي ... 3-الوثائق المصنفة: أي مكتوب ورقي أو إلكتروني أو رسم أو مخطط أو خريطة أو صورة أو شريط صوتي أو سمعي بصري أو أي سند مادي أو إلكتروني آخر كانت محل تدابير ترمي إلى منع نشرها أو تقييد الاطلاع عليها. 4-المعلومات: أي حدث أو خبر مهما كان مصدره، وثقة أو صورة أو شريط صوتي أو مرئي أو سمعي بصري أو محادثة أو مكالمة هاتفية، يؤدي الكشف عنها إلى المساس بالسلطات المعنية**»

في حين تنص المادة (6) من الأمر نفسه على أنه: «**تصنف الوثائق حسب درجة حساسيتها، إلى الأصناف الآتية:**

-"سري جدا"، ويتضمن الوثائق التي يلحق إفشاؤها خطرا بالأمن الوطني الداخلي والخارجي،

-"سري"، ويتضمن الوثائق التي يلحق إفشاؤها ضررا خطيرا بمصالح الدولة،

-"واجب الكتمان"، ويتضمن الوثائق التي يلحق إفشاؤها ضررا أكيدا بمصالح الحكومة أو الوزارات أو الإدارات أو إحدى الهيئات العمومية،

-"توزيع محدود" ويتضمن الوثائق التي إفشاؤها إلى المساس بمصالح الدولة ولا يجوز الاطلاع عليها إلا من قبل الأشخاص المؤهلين بحكم الوظيفة أو المهمة.

تحدد شروط وكيفيات تطبيق هذه المادة عن طريق التنظيم».

أ- صفة الجاني:

يقصد بالتدقيق حسب المادة (16/2) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين: **«التحقق من مدى المطابقة وفقا لمرجعية ما»**، كما حدد القانون نفسه السلطات التي يمكنها إجراء عمليات التدقيق والمتمثلة في السلطة الوطنية وفقا للمادة (5/18) [1] منه، كما خول هذه الصلاحية أيضا للسلطة الحكومية بموجب المادة (6/28) [2]، ويكون ذلك على مستوى الطرف الثالث الموثوق، أما عن السلطة الاقتصادية فقد خولها هي الأخرى صلاحية التدقيق من خلال مكاتب معتمدة وذلك وفقا للمادة (8/30) [3] من القانون نفسه، كما حدد المشرع الجزائري مفهوم الموظف العمومي المنصوص عليه في الأمر رقم (21-09) المذكور أعلاه، من خلال المادة (3) من الأمر نفسه[4].

---

(1)- تنص المادة (18 ف5) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين على أنه: **«تكلف السلطة بترقية استعمال التوقيع والتصديق الإلكترونيين وتطويرهما وضمان موثوقية استعمالهما.**

وفي هذا الإطار، تتولى المهام الآتية: ...

5-القيام بعمليات التدقيق على مستوى السلطتين الحكومية والاقتصادية للتصديق الإلكتروني، عن طريق الهيئة الحكومية المكلفة بالتدقيق...»

(2)- تنص المادة (28 ف 6) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين على أنه: **«تكلف السلطة الحكومية للتصديق الإلكتروني بمتابعة ومراقبة نشاط التصديق الإلكتروني للأطراف الثلاثة الموثوقة، وكذلك توفير خدمات التصديق الإلكتروني لفائدة المتدخلين في الفرع الحكومي.**

وفي هذا الإطار، تتولى المهام الآتية: ...

6-القيام بعمليات التدقيق على مستوى الطرف الثالث الموثوق، عن طريق الهيئة الحكومية المكلفة بالتدقيق، طبقا لسياسة التصديق».

(3)- تنص المادة (30 ف 8) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين على أنه: **«تكلف السلطة الاقتصادية للتصديق الإلكتروني بمتابعة ومراقبة مؤدي خدمات التصديق الإلكتروني الذين يقدمون خدمات التوقيع والتصديق الإلكترونيين لصالح الجمهور.**

وفي هذا الإطار، تتولى المهام الآتية: ...

8-التحقق من مطابقة طالبي التراخيص مع سياسة التصديق الإلكتروني بنفسها أو عن طريق مكاتب تدقيق معتمدة، ...»

(4)- تنص المادة (3) من الأمر (21-09) المتعلق بحماية المعلومات والوثائق الإدارية، على أنه: **«يقصد في مفهوم هذا الأمر، بما يأتي:**

1-الموظف العمومي: =

نلاحظ من المواد أعلاه، أن علة التجريم هنا تكمن في أن الجاني قد أؤتمن على المعلومات والبيانات بسبب وظيفته، لذا فقد حدد المشرع الجزائري العقوبة بالنظر إلى الخطورة البالغة لجرائم إفشاء السر المهني.

ب- الركن المادي للجريمة:

يتحقق الركن المادي في هذه الجريمة بكشف المكلف بالتدقيق أو الموظف العمومي عن المعلومات السرية التي اطلع عليها بحكم وظيفته للغير، ولم يبين المشرع الجزائري في هذه الجريمة نوع البيانات التي خصّها بالحماية فيما إذا كانت تتعلق بالتوقيع الإلكتروني، أو شهادة التصديق أو غيرها من المعلومات السرية، وعليه فأي معلومة سرية يفشيها المكلف بالتدقيق ويكون قد اطلع عليها بحكم وظيفته تحقق قيام الركن المادي لهذه الجريمة.

ج-الركن المعنوي للجريمة:

جريمة كشف معلومات التوقيع الإلكتروني أثناء التدقيق، جريمة عمدية تتطلب قصدا جنائيا عاما بعنصريه العلم والإرادة، إذ يجب أن يعلم الجاني أنه يقوم بالكشف عن البيانات السرية التي اطلع عليها بحكم وظيفته، مع اجاه ارادته إلى ارتكاب هذا الفعل الإجرامي، ولا تشترط هذه الجريمة قصدا جنائيا خاصا، حيث لا يهم القصد أو الباعث هنا من وراء افشاء هذه البيانات.

=-كل شخص يشغل منصبا تشريعيا أو تنفيذيا أو إداريا أو قضائيا أو في أحد المجالس الشعبية المحلية المنتخبة، سواء أكان معينا أو منتخبا، دائما أو مؤقتا، مدفوع الأجر أو غير مدفوع الأجر، بصرف النظر عن رتبته أو أقدميته،

-كل شخص آخر يتولى، ولو مؤقتا، وظيفة أو وكالة بأجر أو بدون أجر، ويساهم بهذه الصفة في خدمة هيئة عمومية أو مؤسسة عمومية أو أي مؤسسة أخرى تملك الدولة كل أو بعض رأسمالها، أو أي مؤسسة أخرى تقدم خدمة عمومية،

-كل شخص آخر معرف بأنه موظف عمومي أو من في حكمه طبقا للتشريع والتنظيم المعمول بهما».

د-العقوبة المقررة لجريمة كشف معلومات سرية أثناء التدقيق:

يعاقب المكلف بالتدقيق الذي ارتكب جريمة افشاء بيانات سرية أثناء التدقيق بالحبس من ثلاثة (3) أشهر إلى سنتين (2) وبغرامة من عشرين ألف دينار (20.000 دج) إلى مائتي ألف دينار (200.000 دج) أو بإحدى هاتين العقوبتين فقط، وفقا لنص المادة (73) أعلاه.

في حين يعاقب الموظف العمومي الذي يفشي معلومات أو وثائق مصنفة بعقوبات تتراوح فيما بين ستة (6) أشهر إلى غاية خس (5) سنوات وفقا لتصنيف الوثيقة المسربة ودرجة خطورة الفعل، كما أوضحناه من خلال المادتين (28) و(29) من الأمر رقم (21-09) السالف ذكره.

ثانيا: جرائم إساءة استخدام شهادة التصديق الإلكتروني

يقع الإضرار بشهادة التصديق الإلكتروني في حال الإدلاء بإقرارات كاذبة لأجل الحصول على الشهادة، وكذا في حال استخدام هذه الشهادة لأغراض غير مشروعة، وقد تدخل المشرع الجزائري لتجريم هذين الفعلين بموجب المادتين (66) و (74)[1] من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين سالف الذكر، وسنفصل في كل جريمة على حدى.

1- جريمة الإدلاء بإقرارات كاذبة:

يقدم المعني بالحصول على توقيع إلكتروني مجموعة من البيانات والإقرارات لمؤدي خدمات التصديق الإلكتروني من أجل الحصول على شهادة التصديق الإلكتروني، هذه

---

(1)- تنص المادة (66) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين على أنه: **«يعاقب بالحبس من ثلاثة (3) أشهر إلى ثلاث (3) سنوات وبغرامة من عشرين ألف دينار (20.000دج) إلى مائتي ألف دينار (200.000 دج) أو بإحدى هاتين العقوبتين فقط، كل من أدلى بإقرارات كاذبة للحصول على شهادة تصديق إلكتروني موصوفة»**

تنص المادة (74) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين على أنه: **«يعاقب بغرامة من ألفي دينار (2000 دج) إلى مائتي ألف دينار (200.000 دج) كل شخص يستعمل شهادته للتصديق الإلكتروني الموصوفة لغير الأغراض التي منحت لأجلها».**

المعلومات والبيانات التي يحتمل أن تكون غير صحيحة، ما أدى بالمشرع إلى تجريم الإدلاء بإقرارات كاذبة، وهي جريمة تقع على البيانات والمعلومات التي تتضمنها شهادة التصديق.

نص المشرع الجزائري على هذه الجريمة في نص المادة (66) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين: «... **كل من أدلى بإقرارات كاذبة للحصول على شهادة تصديق إلكتروني موصوفة»**، وهدف المشرع الجزائري من تجريمها هو حماية المتعاملين في نطاق المعاملات الإلكترونية من البيانات الخاطئة وزيادة الثقة فيما بينهم والحفاظ على حقوقهم [1].

أ- الركن المادي للجريمة:

تتحقق هذه الجريمة بالتصريح بإقرارات كاذبة لدى جهات التصديق الإلكتروني، ويشترط في البيانات المدلى بها إلى مؤدي خدمات التصديق الإلكتروني أن تكون غير صحيحة بغرض الحصول على شهادة تصديق إلكتروني موصوفة، ذلك أن هذه الأخيرة عبارة عن وثيقة في شكل إلكتروني تثبت الصلة بين بيانات التحقق من التوقيع الإلكتروني والموقّع، وهي تمنح من قبل مؤدّي خدمات التصديق الإلكتروني لصاحبها وذلك بعد التحقّق من بيانات التحقق الإلكتروني، كما لا يشترط أن تكون جميع البيانات المدلى بها خاطئة، فيكفي لقيام الجريمة الإدلاء بأحد البيانات غير الصحيحة فقط، حتى و لو كانت باقي البيانات صحيحة.

لم يتضمن نص المادة (66) طريقة الإدلاء بالبيانات الخاطئة، سواء أدلى بها صاحبها شفهيا أو تم تقديمها في أوراق مكتوبة أو في دعامة إلكترونية تتضمنها، على أن يتم الإدلاء بهذه البيانات وجوبا إلى جهة تصديق إلكتروني.

(1)- عبد الفتا بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، مرجع سابق، ص496.

وعليه، فجريمة الإدلاء بإقرارات كاذبة تُعد من قبيل جرائم السلوك المجرد، بمعنى أن المشرع لا يشترط لقيام الركن المادي فيها حصول ضرر معيّن، وإنما يكفي تحقّق النشاط الإجرامي وهو التصريح بإقرارات كاذبة [1].

ب- الركن المعنوي للجريمة:

يتمثل الركن المعنوي لهذه الجريمة في القصد الجنائي العام بعنصريه العلم والإرادة، يتحقّق بعلم الجاني أو ممثله القانوني بأنه يدلي بمعلومات ينبغي عليه تقديمها صحيحة، أيا كان موضوع المعلومات، سواء كانت تتعلق بهوية صاحب الشهادة أو بهوية الشخص المفوض. ورغم ذلك يخالف الالتزام الملقى على عاتقه، لغرض الحصول على شهادة تصديق إلكتروني، وأن تنصرف إرادته إلى ارتكاب السلوك الإجرامي المتمثل في الإدلاء بإقرارات كاذبة مع قبوله النتيجة المترتبة على فعله بوصفه محظور قانونا.

مع ذلك يجب توفر قصد جنائي خاص لدى الجاني، وهو أن تتجه نيته للحصول على شهادة تصديق إلكتروني، إلى جانب القصد الجاني العام بعنصريه.

ج- العقوبة المقررة لجريمة الإدلاء بإقرارات كاذبة:

يترتب على تحقق أركان جريمة الإدلاء بإقرارات كاذبة، معاقبة الجاني حسب نص المادة (66) من القانون رقم (15-04) المتعلق التوقيع والتصديق الإلكترونيين، بالحبس من ثلاثة (3) أشهر إلى ثلاث (3) سنوات، وبغرامة من عشرين ألف دينار (20.000 دج) إلى مائتي ألف دينار (200.000 دج) أو بإحدى هاتين العقوبتين فقط.

هذا إذا كان الجاني شخص طبيعي، أما إذا كان شخص معنوي فتضاعف العقوبة المذكورة أعلاه حسب نص المادة (75) من القانون السالف الذكر إلى الغرامة المقدرة خمس مرات الحد الأقصى للغرامة المنصوص عليها بالنسبة للشخص الطبيعي، وعليه تكون العقوبة الغرامة المقدرة ب (1.000.000 دج).

---

(1)- شنين صالح، مرجع سابق، ص 181.

2- جريمة الاستخدام غير المشروع لشهادة التصديق الإلكتروني:

جرّم المشرع الجزائري بموجب المادة (74) من القانون رقم (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين، كل من يستعمل شهادة تصديق إلكتروني موصوفة خاصة به لكن لغير الأغراض التي منحت لأجلها، حيث تنص المادة السالفة الذكر على أنه: «**يعاقب بغرامة من ألفي دينار (2000دج) إلى مائتي ألف دينار (200.000دج) كل شخص يستعمل شهادته للتصديق الإلكتروني الموصوفة لغير الأغراض التي منحت من أجلها**»، وعليه تقوم جريمة الاستخدام غير المشروع لشهادة التصديق الإلكتروني على ركنيين مادي ومعنوي نبينهما فيما يلي.

أ- الركن المادي للجريمة:

يتمثل الركن المادي لهذه الجريمة في إتيان الجاني سلوك إيجابي، وهو استعمال شهادة التصديق الإلكتروني الموصوفة لغير الأغراض التي منحت لأجلها، ووفقا لما تقرره المادة (15ف3/ط، ي) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين السالف ذكره، التي بينت أن هناك حدود لاستعمال شهادة التصديق الإلكتروني[1]، غير أنها لم توضح هذه الحدود.

ما يفهم منه أن شهادة التصديق الإلكتروني تستخدم في المجالات المرخص لها قانونا باستعمالها، فإذا ما استعملها صاحبها في غير هذه الحالات نكون أمام جريمة استعمال بطريقة غير شرعية، كاستعمال شهادة التصديق الإلكتروني في معاملات محظورة قانونا، كمعاملة مثلا لشراء المخدرات، أو لعب القمار عبر الانترنت وغيرها.

---

(1)- تنص المادة (15 ف3/ط) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين على أنه: «**شهادة التصديق الإلكتروني الموصوفة هي شهادة تصديق إلكتروني تتوفر فيها المتطلبات التالية: ...**

3- يجب أن تتضمن على الخصوص: ...

ط- حدود استعمال شهادة التصديق الإلكتروني، عند الاقتضاء،

ي-حدود قيمة المعاملات التي قد تستعمل من أجلها شهادة التصديق الإلكتروني، عند الاقتضاء ...».

ب- **الركن المعنوي للجريمة:**

مضمون الركن المعنوي لهذه الجريمة يتضمن في القصد الجاني العام بعنصرية العلم والإرادة، ويتحقق العلم عندما يعلم الجاني أنه يتجاوز الحدود المفروضة على استعمال شهادته أو الحد الأقصى لقيمة المعاملات التي يمكن أن تستعمل بها الشهادة، وأن تتجه إرادته إلى إتيان هذا السلوك المجرّم.

كما لا يشترط توفر القصد الجاني الخاص المتمثل في نية الإضرار بالغير لقيام هذه الجريمة، لأنه بمجرد الانحراف في استعمال الشهادة لغير الغرض الذي منحت لأجله تقوم هذه الجريمة، وفي حالة حدوث الضرر للغير يتحمل المسؤولية صاحب الشهادة ويستثنى منها مؤدي خدمات التصديق الإلكتروني وفقا للمادتين (56 و57)[1] من القانون رقم (15-04) السالف الذكر.

ج-العقوبة المقررة لجريمة الاستخدام غير المشروع لشهادة التصديق الإلكتروني:

يعاقب الشخص الطبيعي حسب نص المادة (74) من القانون رقم (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين، بغرامة من ألفي دينار (2.000 دج) إلى مائتي ألف دينار (200.000 دج) إذا ما استعمل شهادة للتصديق الإلكتروني الموصوفة لغير الأغراض التي منحت من أجلها. وتضاعف العقوبة المذكورة أعلاه خمس (5) مرات الحد الأقصى المنصوص عليه بالنسبة للشخص الطبيعي، إذا كان مرتكب جنحة الاستعمال غير الشرعي لشهادة

---

(1)- تنص المادة (56) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين، على أنه: **«يمكن مؤدي خدمات التصديق الإلكتروني، أن يشير، في شهادة التصديق الإلكتروني الموصوفة، إلى الحد الأقصى لقيمة المعاملات التي يمكن أن تستعمل في حدودها هذه الشهادة، بشرط أن تكون هذه الإشارة واضحة ومفهومة من طرف الغير. وفي هذه الحالة، لا يكون مؤدي خدمات التصديق الإلكتروني مسؤولا عن الضرر الناتج عن تجاوز ذلك الحد الأقصى».**

تنص المادة (57) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين، على أنه: **«لا يكون مؤدي خدمات التصديق الإلكتروني مسؤولا عن الضرر الناتج عن عدم احترام صاحب شهادة التصديق الإلكتروني الموصوفة لشروط استعمال بيانات إنشاء التوقيع الإلكتروني».**

التصديق الإلكتروني الموصوفة شخص معنوي وفقا لنص المادة (75) من القانون نفسه، وعليه فالغرامة تقدر بمليون دينار (1.000.000 دج).

الفرع الثاني

الجرائم الماسة بنشاط التصديق الإلكتروني

فرض المشرع الجزائري على مؤدّي خدمات التصديق الإلكتروني مجموعة من الالتزامات ذات صلة مباشرة بتنفيذ نشاطاتهم المرتبطة بعملية التصديق الإلكتروني، تتمثل أساسا في حصوله على شهادة الترخيص التي تأهله للممارسة نشاط التصديق الإلكتروني والتي نص عليها في المواد من (33) إلى (40) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين، كما فرض عليه واجبات عديدة منصوص عليها في المواد من (53) إلى (60) من القانون نفسه.

فإذا ما أخل مؤدّي خدمات التصديق الإلكتروني بأحد الالتزامات أو الواجبات المفروضة عليه بمناسبة تأدية نشاطه، تعرّض للمساءلة الجزائية وردت في صورة جرائم على سبيل الحصر في القانون (15-04) سالف الذكر، والتي تتمّثل في جريمة عدم تحديد هوية طالب شهادة التصديق الإلكتروني **(أولا)**، جريمة عدم إبلاغ السلطة الاقتصادية بالتوقف عن النشاط **(ثانيا)**، جريمة ممارسة نشاط التصديق الإلكتروني بدون ترخيص **(ثالثا)**.

أولا: جريمة عدم تحديد هوية طالب شهادة التصديق

بالرجوع إلى أحكام المادة (44) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونين السالف الذكر[1]، يتبين أن المشرع الجزائري فرض على مؤدي خدمات التصديق

(1)- تنص المادة (44) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين على أنه: «**يجب على مؤدي خدمات التصديق الإلكتروني، قبل منح شهادة التصديق الإلكتروني، أن يتحقق من تكامل بيانات الإنشاء مع بيانات التحقق من التوقيع.**

يمنح مؤدي خدمات التصديق الإلكتروني شهادة أو أكثر لكل شخص يقدم طلبا وذلك بعد التحقق من هويته، وعند الاقتضاء، التحقق من صفاته الخاصة

مجموعة من الالتزامات، وذلك في إطار ممارسته لمهامه، ولعل أهم هذه الالتزامات؛ الالتزام بتحديد هوية طالب شهادة التصديق، سواء كان شخصا طبيعيا أو معنويا، وعند الاقتضاء التحقق أيضا من صفاته الخاصة.

ومن ثم فإن أي إخلال بهذا الالتزام يعتبر جريمة يترتب عنه المسؤولية الجزائية طبقا لأحكام المادة (69) من القانون نفسه[1]، وتقوم جريمة عدم تحديد هوية طالب شهادة التصديق على ركنيين أساسيين –مادي ومعنوي– كغيرها من الجرائم نوضحهما على النحو التالي.

1- الركن المادي للجريمة:

يتمثل الركن المادي في إخلال مؤدي خدمات التصديق الإلكتروني (باعتباره المكلف بإصدار هذه الشهادات لطالبها)، بالتزام تحديد هوية طالب شهادة التصديق الإلكتروني الموصوفة، حسب الفقرة الثانية من المادة (44) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين، كونه المعني والملتزم بالتحقق من بيانات الشهادة.

وكما سبق تبيانه، فقد يكون صاحب شهادة التصديق الإلكتروني شخصا طبيعيا أو معنويا، وفقا لنص المادة (14) من القانون نفسه، لذلك فإن تحديد الهوية يأخذ صورتين؛ الأولى هي التحقق من هوية الشخص الطبيعي، وعند الاقتضاء التحقّق من صفاته الخاصة، والثانية التحقق من الشخص المعنوي عن طريق احتفاظ مؤدي خدمات التصديق الإلكتروني بسجل يدون فيه هوية وصفة الممثل القانوني للشخص المعنوي المستعمل للتوقيع الإلكتروني المتعلق بشهادة التصديق الإلكتروني الموصوفة، بحيث يمكن تحديد هوية الشخص الطبيعي

وفيما يخص الأشخاص المعنوية، يحتفظ مؤدي خدمات التصديق الإلكتروني بسجل يدون فيه هوية وصفة الممثل القانوني للشخص المعنوي المستعمل للتوقيع المتعلق بشهادة التصديق الإلكتروني الموصوفة، بحيث يمكن تحديد هوية الشخص الطبيعي عند كل استعمال لهذا التوقيع الإلكتروني».

(1)- تنص المادة (69) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين على أنه: **«يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من عشرين ألف (20.000 دج) إلى مائتي ألف دينار (200.000 دج) أو بإحدى هاتين العقوبتين فقط كل من يخل عمدا بالتزام تحديد هوية طالب شهادة تصديق إلكتروني موصوفة».**

عند كل استعمال لهذا التوقيع الإلكتروني، وهذا وفقا لنص المادة (44 فـ2) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين، السالف الذكر.

الهدف من تجريم المشرع الجزائري لهذه الأفعال يرجع بالأساس، إلى ما تشكله شهادة تصديق إلكتروني من أهمية بالغة في المعاملات الإلكترونية، وهذا لما تحتويه من بيانات ومعلومات سرية من شأن أي استعمال غير مشروع لها من غير ذي صفة (صاحب شهادة التصديق الإلكتروني) الإضرار بالمعاملات الإلكترونية التي تستوجب الثقة والأمان.

2- الركن المعنوي للجريمة:

تعتبر جريمة الإخلال بالتزام تحديد هوية طالب شهادة التصديق الإلكتروني من الجرائم العمدية التي تستلزم توافر القصد الجنائي العام بصورتيه العلم والإرادة، إذ يجب أن يعلم مؤدي خدمات التصديق الإلكتروني بإخلاله بالتزامه المتمثل في تحديد هوية طالب شهادة تصديق إلكتروني موصوفة والتحقق منها، وهذا الفعل يجّرمه القانون، كما يجب أن تتّجه إرادته إلى إتيان هذا الفعل.

ولم يتطلب المشرع أيضا في هذه الجريمة القصد الجنائي الخاص، بل تقوم بمجرد توافر القصد الجنائي العام بعنصرية العلم والإرادة، إلى جانب الركن المادي للجريمة.

3- العقوبة المقررة لجريمة عدم تحديد هوية طالب شهادة التصديق:

يترّتب على تحقق الركنين السالف ذكرهما، قيام جريمة الإخلال بالتزام تحديد هوية طالب شهادة التصديق الإلكتروني الموصوفة، والتي تعاقب عليها المادة (69) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين، بالحبس من شهرين إلى ثلاثة (3) سنوات، وبغرامة مالية من عشرين ألف دينار (20.000 دج) إلى مائتي ألف دينار (200.000 دج)، أو بإحدى هاتين العقوبتين فقط، وعليه للقاضي السلطة التقديرية في معاقبة مؤدي خدمات التصديق الإلكتروني بالحبس والغرامة أو معاقبته بإحدى العقوبتين فقط.

أما في حالة ما إذا كان الجاني شخصا معنويا فيعاقب بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المنصوص عليها بالنسبة للشخص الطبيعي، أي أنها تقدر بمليون دينار (1.000.000 دج) حسب نص المادة (75) من القانون نفسه.

ثانيا: جريمة عدم إبلاغ السلطة الاقتصادية بالتوقف عن النشاط

ألزم المشرع الجزائري السلطة الاقتصادية للتصديق الإلكتروني مهمة منح تراخيص لمؤدي خدمات التصديق الإلكتروني، وكذا العمل على متابعة ومراقبة نشاطهم، وفي مقابل ذلك يقع على عاتق مؤدي خدمات التصديق الإلكتروني التزام اتجاه هذه السلطة الاقتصادية بضرورة إعلامها بالتوقّف عن نشاط التصديق الإلكتروني في الآجال المحددة في سياسة التصديق لهذه السلطة وفقا لما جاءت به كل من المادتين (58 و59)[1] من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين.

وبهذا يتضح أن كل سلوك سلبي لعدم إعلام عن التوقف عن النشاط يشكل جريمة وفقا لنص المادة (67) من القانون (15-04) والتي تنص على أنه: «**يعاقب بالحبس من شهرين (2) إلى سنة (1) واحدة وبغرامة من مائتي ألف دينار (200.000دج) إلى مليون دينار (1000.000دج)، او بإحدى هاتين العقوبتين فقط، كل مؤدي خدمات التصديق الإلكتروني**

---

(1)- تنص المادة (58) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين على أنه: «**يجب على مؤدي خدمات التصديق الإلكتروني، إعلام السلطة الاقتصادية للتصديق الإلكتروني، في الآجال المحددة في سياسة التصديق لهذه السلطة، برغبته في وقف نشاطاته المتعلقة بتأدية خدمات التصديق الإلكتروني أو بأي فعل قد يؤدي إلى ذلك.**

وفي هذه الحالة، يلتزم مؤدي خدمات التصديق الإلكتروني بأحكام سياسة التصديق للسلطة الاقتصادية للتصديق الإلكتروني المتعلقة باستمرارية الخدمة.

يترتب على وقف النشاط سحب الترخيص».

وتنص المادة (59) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين على أنه: «**يجب على مؤدي خدمات التصديق الإلكتروني الذي يوقف نشاطه لأسباب خارجة عن إرادته أن يعلم السلطة الاقتصادية للتصديق الإلكتروني بذلك فورا، وتقوم هذه الأخيرة بإلغاء شهادته للتصديق الإلكتروني الموصوفة بعد تقدير الأسباب المقدمة.**

وفي هذه الحالة، يتخذ مؤدي الخدمات التدابير اللازمة والمنصوص عليها في سياسة التصديق الإلكتروني للسلطة الاقتصادية، من أجل حفظ المعلومات المرتبطة بشهادة التصديق الإلكتروني الموصوفة الممنوحة له».

أخل بالتزام إعلام السلطة الاقتصادية بالتوقف عن نشاطه في الآجال المحددة في المادتين 58 و59 من هذا القانون». وسنوضح فيما يلي أركان هذه الجريمة.

1- الركن المادي للجريمة:

يتحقّق السلوك المادي لهذه الجريمة بتوقّف مؤدّي خدمات التصديق الإلكتروني والمرخص له من الهيئة الاقتصادية للتصديق الإلكتروني [1]، عن نشاط التصديق الالكتروني دون إعلام هذه الهيئة في الآجال المحددة في سياسة التصديق للسلطة الاقتصادية. وعليه يتضح أن النشاط الاجرامي يتمثل في مجرد عدم الإبلاغ عن التوقف عن النشاط، دون أن يتطلب تحقق نتيجة معينة.

وباستقراء نص المادة (58) سالفة الذكر، نجدها تنص على حالة التوقّف الارادي عن مزاولة النشاط، بحيث يلزم في هذه الحالة مؤدّي خدمات التصديق بإعلام السلطة الاقتصادية ضمن الآجال المحددة في سياسة التصديق عن رغبته في التوقف عن ممارسة نشاطاته المتعلقة بتأدية خدمات التصديق الإلكتروني، ذلك أن مقدم خدمات التصديق ملزم بضمان ديمومة واستمرارية الخدمات المقدمة من طرفه طيلة مدة مباشرة النشاط، ما لم يسحب منه الترخيص.

في حين تطرق المشرع الجزائري من خلال المادة (59) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين سالفة الذكر، لحالة التوقف اللاإرادي، حيث تلزم مؤدي خدمات التصديق الالكتروني في حال توقف نشاطه لأسباب خارجة عن إرادته بإعلام السلطة الاقتصادية بذلك التوقف فورا، لتقوم هذه الأخيرة وبعد تقديريها للأسباب المقدمة، بإلغاء شهادة التصديق الإلكتروني الخاصة به، ويلتزم مؤدي خدمات التصديق الإلكتروني في هذه الحالة باتخاذ جميع التدابير اللازمة من أجل حفظ المعلومات المرتبطة بشهادة التصديق الإلكتروني الموصوفة الممنوحة له.

---

(1)- تنص المادة (33) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين، على أنه: **«يخضع نشاط تأدية خدمات التصديق الإلكتروني إلى ترخيص تمنحه السلطة الاقتصادية للتصديق الإلكتروني».**

وتبلغ مدة الترخيص الممنوح لمؤدي خدمات التصديق الإلكتروني (5) سنوات قابلة للتجديد بحسب نص المادة (40) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين، وبالتالي فإن أي توقف عن النشاط قبل انتهاء هذه المدة القانونية سواء لأسباب إرادية أو غير إرادية من قبل مؤدي خدمات التصديق الإلكتروني دون إعلام السلطة الاقتصادية للتصديق الالكتروني تضعهم تحت المسؤولية الجزائية.

الملاحظ كذلك أن العقوبة المنصوص عليها في المادة (67)[1] من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين، تطال مؤدي خدمات التصديق الإلكتروني في حال عدم إبلاغه السلطة الاقتصادية بالتوقف عن النشاط فقط، غير أنها لم تتطرق للالتزامات الأخرى المنصوص عليها بموجب المادتين (58 و59) السالفتي الذكر؛ المتعلقة بضمان استمرار الخدمة، وحفظ المعلومات المرتبطة بشهادة التصديق الإلكتروني الموصوفة.

2- الركن المعنوي للجريمة:

تعتبر جريمة عدم إبلاغ السلطة الاقتصادية بالتوقف عن النشاط، من الجرائم العمدية لا بد من أن تتوفر فيها القصد العام بعنصريه العلم والإرادة، فيجب أن الجاني -مؤدي خدمات التصديق الإلكتروني- عالما بإخلاله بالتزام إبلاغ السلطة الاقتصادية بوقف نشاطه في الآجال المحددة وفقا للمادتين (58 و59) من القانون (15-04) سالف الذكر، واتجاه ارادته إلى ارتكاب هذه الجريمة.

واكتفى المشرع في هذه الجريمة كبقية الجرائم الأخرى بالقصد الجنائي العام، ولا عبرة للقصد الخاص الذي دفع الجاني للإخلال بهذا الالتزام.

---

(1)- تنص المادة (67) من القانون (15-04) سالف الذكر، على أنه: **«يعاقب بالحبس من شهرين (2) إلى سنة (1) واحدة وبغرامة من مائتي ألف دينار (200.000دج) إلى مليون دينار (1000.000دج)، او بإحدى هاتين العقوبتين فقط، كل مؤدي خدمات التصديق الإلكتروني أخل بالتزام إعلام السلطة الاقتصادية بالتوقف عن نشاطه في الآجال المحددة في المادتين 58 و59 من هذا القانون».**

3- العقوبة المقررة لجريمة عدم إبلاغ السلطة الاقتصادية بالتوقف عن النشاط:

عاقب المشرع الجزائري مؤدي خدمات التصديق الإلكتروني -الشخص الطبيعي- المرتكب لجريمة عدم ابلاغ السلطة الاقتصادية بالتوقف عن النشاط، وفقا للمادة (67) من القانون (15-04) بالحبس من شهرين إلى سنة واحدة، وبغرامة من مائتي ألف دينار (200.000 دج) إلى مليون دينار (1.000.000 دج)، أو بإحدى هاتين العقوبتين فقط.

أما بالنسبة للشخص المعنوي فالعقوبة هي الغرامة التي تعادل (5) مرات الحد الأقصى للغرامة المنصوص عليها في المادة (67)، وعليه تكون الغرامة المقررة للشخص المعنوي حسب المادة (75) من القانون (15-04) سالف الذكر، خمسة مليون دينار (5.000.000دج).

ثالثا: جريمة ممارسة نشاط التصديق الإلكتروني بدون ترخيص

لا يمكن لمؤدي خدمات التصديق الإلكتروني ممارسة نشاطه إلا بعد حصوله على الترخيص من قبل السلطة الاقتصادية للتصديق الإلكتروني[1]، ونظرا لأهمية التصديق الإلكتروني في تأمين المعاملات الإلكترونية، جرّم المشرع الجزائري مزاولة نشاط التصديق الإلكتروني بدون الحصول على ترخيص مسبق، أو استئناف، أو مواصلة مؤدّي خدمات التصديق الإلكتروني لنشاطه بعد سحب الترخيص منه، وفقا لما تنص عليه المادة (72) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين التي تقضي بأنه: «**يعاقب بالحبس من سنة (1) واحدة إلى ثلاث (3) سنوات، وبغرامة من مائتي ألف دينار (200.000 دج) إلى مليوني دينار (2.000.000 دج) أو بإحدى هاتين العقوبتين فقط، كل من يؤدي خدمات التصديق الإلكتروني للجمهور دون ترخيص أو كل مؤدي خدمات التصديق الإلكتروني يستأنف أو يواصل نشاطه بالرغم من سحب ترخيص.**

تصادر التجهيزات التي استعملت لارتكاب الجريمة طبقا للتشريع المعمول به».

---

(1)- تنص المادة 33 من القانون 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين على أنه: «**يخضع نشاط تأدية خدمات التصديق الإلكتروني إلى ترخيص تمنحه السلطة الاقتصادية للتصديق الإلكتروني**».

وعليه تقوم جريمة مزاولة نشاط التصديق الإلكتروني دون ترخيص على ركنين أساسين نوضحهما فيما يلي.

1- الركن المادي للجريمة:

يتحقق السلوك الاجرامي في جريمة مزاولة نشاط التصديق الإلكتروني بدون ترخيص في صورتين، نصت عليهما المادة (72) من القانون (15-04) السالف ذكره وهما:

- انتحال الجاني صفة مؤدي خدمات التصديق الإلكتروني ومباشرته لنشاط التصديق الإلكتروني دون حصوله على ترخيص من السلطة المختصة.
- استئناف او مواصلة مؤدي خدمات التصديق الإلكتروني النشاط بالرغم من سحب الترخيص.

وعليه يتمثل السلوك الإجرامي المكوّن للركن المادي في جريمة مزاولة نشاط التصديق الإلكتروني بدون ترخيص في انتحال الجاني صفة مؤدي خدمات التصديق الإلكتروني المرخص له من قبل السلطة الاقتصادية، أو قد يتمثل السلوك الثاني في مواصلة مؤدي خدمات التصديق الإلكتروني لنشاطه على الرغم من سحب الترخيص الممنوح له مسبقا، وبهذا تعتبر كل عمليات المصادقة الإلكترونية التي تتم في هذه الفترة غير قانونية وترتب المسؤولية الجنائية في حق مؤدي الخدمات [1].

السبب في تجريم هذا الفعل هو الآثار الخطيرة المترتبة على شهادة التصديق الإلكتروني في حق الغير، حيث يكون مضمونها التسليم بصحة بيانات التوقيع الإلكتروني أو بيانات المعاملة المطلوب صدور شهادة التصديق حولها [2].

---

(1)- صحراوي مصطفى، الحماية الجزائية للتوقيع والتصديق الإلكترونيين في التشريع الجزائري، أطروحة مقدمة لنيل شهادة دكتوراه " ل.م.د"، في العلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة وهران 2، 2021/2020، ص 116.

(2)- بن قارة مصطفى عائشة، الحماية الجنائية للحكومة الإلكترونية دراسة مقارنة، أطروحة مقدمة لنيل شهادة دكتوراه " علوم، تخصص قانون عام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2018/2017، ص 146.

وتدخل جريمة مزاولة نشاط التصديق الإلكتروني بدون رخصة في نطاق جرائم الخطر، التي يكتمل الركن المادي فيها بمجرد اقتراف الجاني لسلوك مزاولة النشاط بدون رخصة، ولا يشترط تحقق نتيجة معينة ولو لم يصب المجني عليه ضرر فعلي.

2- الركن المعنوي للجريمة:

تُعد جريمة مزاولة نشاط التصديق الإلكتروني بدون ترخيص من الجرائم العمدية التي لا بد فيها من توافر القصد الجنائي العام، الذي يقوم على عنصري العلم والإرادة؛ إذ ينبغي أن يعلم الجاني بأنه يقوم بمزاولة نشاط التصديق الإلكتروني بدون ترخيص في حالة كان من الغير، أو أن يعلم بأنه استأنف أو واصل نشاط التصديق الإلكتروني على الرغم من سحب الترخيص منه، هذا بالنسبة لمؤدي خدمات التصديق الإلكتروني، وفي كلتا الحالتين تتجه إرادتهما إلى اقتراف الفعل المُجرَم، ومن ثمة لا يتصور وقوع هذه الجريمة بطريق الخطأ.

3- العقوبة المقررة لجريمة ممارسة نشاط التصديق الإلكتروني بدون ترخيص:

يترتب على قيام جريمة مزاولة نشاط التصديق الإلكتروني دون ترخيص أو بعد سحبه العقوبة المنصوص عليها بموجب المادة (72) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين.

حيث قرر المشرع الجزائري لهذه الجريمة عقوبة أصلية تتمثل في الحبس من سنة (1) واحدة إلى ثلاث (3) سنوات، وبغرامة من مائتي ألف دينار (200.000 دج) إلى مليوني دينار (2.000.000 دج) أو بإحدى هاتين العقوبتين فقط.

أما عن العقوبة التكميلية فتتمثل في مصادرة [1] التجهيزات التي استعملت لارتكاب الجريمة وذلك طبقا للتشريع المعمول به.

(1)- عرفت المادة 15 من قانون العقوبات الجزائري المصادرة بأنها: «**المصادرة هي الأيلولة النهائية إلى الدولة لمال أو مجموعة أموال معينة، أو ما يعادل قيمتها عند الاقتضاء**».

في حين يعاقب الشخص المعنوي طبقا للمادة (75) من القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين السالف ذكره بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المنصوص عليها بالنسبة للشخص الطبيعي، وبالتالي يعاقب في هذه الجريمة بغرامة تقدر بعشر ملايين دينار (10.000.000 دج)، بالإضافة لمصادرة التجهيزات التي استعملت لارتكاب الجريمة.

خلاصة الباب الثاني

خلاصة الباب الثاني

تتسم المعاملات القانونية في صورتها التقليدية بميزتين أساسيتين: تتمثل الأولى في وجود محرر مكتوب على وسيط مادي ليس من السهل التغيير في مضمونه دون ترك أثر، في حين تتمثل الميزة الثانية في ارتباطه بتوقيع يفيد الإقرار بصحة مضمونه ونسبته إلى من وقع عليه، هاتان السمتان اللتان لا وجود لهما بنفس الصورة بالنسبة للمحررات والتواقيع الإلكترونية، مما يثير الشكوك حول درجة الثقة والأمان التي تتوفر عليها، وهو ما ينعكس سلبا على قيمتهما من الناحية القانونية، لأجل ذلك سعت تشريعات الإثبات الإلكتروني الدولية منها والوطنية إلى خلق حماية قانونية تعنى بأدلة الإثبات الإلكتروني.

تتمثل الحماية التي أقرتها تشريعات الإثبات الإلكتروني بصفة عامة، والمشرع الجزائري بصفة خاصة لأدلة الإثبات الإلكتروني في نوعين: حماية تقنية أو قبلية تتعلق بالأمن المعلوماتي وجميع الوسائل الكفيلة بضمان أمن وسرية وصحة المعلومات المتداولة إلكترونيا، وحماية جزائية أو بعدية تقوم على تجريم جميع الاعتداءات الواقعة على أدلة الاثبات الإلكتروني.

تتمثل الاشتراطات القانونية التقنية والفنية التي نصت عليها تشريعات الإثبات الإلكتروني في آليتين اثنتين لا تقل احداهما أهمية عن الأخرى، تتمثل الآلية الأولى في "**التصديق الإلكتروني**" في حين تتمثل الثانية في " **الحفظ الإلكتروني**"، وهما عبارة عن تقنيتين متكاملتين تعملان على ضمان أمن وسلامة المحررات والتواقيع الإلكترونية، مما يمنحهما حجية في الاثبات تعادل حجية المحررات والتواقيع التقليدية.

تعمل آلية التصديق الإلكتروني على تحقيق مجموعة من الأهداف من بينها، تحديد هوية أطراف المعاملة الإلكترونية، وتحديد أهليتهم للتعامل، وكذا ضمان سلامة وسرية محتوى البيانات المتداولة عبر شبكة الانترنت، مع ضمان عدم إنكار للمحررات أو التواقيع الإلكترونية الصادرة من أطراف المعاملة الإلكترونية.

بينما تضمن آلية الحفظ الإلكتروني سلامة المعلومات الواردة في المحرر الإلكتروني من أي تغيير في شكلها الأصلي الذي أنشأت به، أو أرسلت أو استلمت عليه، مع ضمان إمكانية استرجاعه في أي وقت بذات الشكل الذي تم إنشاؤه أو إرساله أو تسلمه عليه، دون أي تحريف أو تبديل أو تغيير.

كما لا تقتصر مواجهة المخاطر التي قد تمس بأدلة الإثبات الإلكتروني على توفير الحماية الوقائية أو ما يطلق عليها بالحماية التقنية أو الفنية، بل وجب أن يكون هذا النظام الأمني مدعما بحماية جزائية للمعاملات الإلكترونية تتصدى لجميع أشكال الاعتداء والجرائم التي قد تقع عليها.

حيث اتخذت الجريمة المعلوماتية صورا عديدة استوجبت معها المواجهة التشريعية، إذ وجدت بعض الجرائم التقليدية تطبيقاً حديثاً لها في حيز المعاملات الإلكترونية الاقتصادية بشكل خاص، كالتزوير الإلكتروني والسرقة الإلكترونية، أين حاولنا تطبيق القواعد العامة للحماية الجزائية على هذه الجرائم، وإسقاط أركان الجريمة في صورتها التقليدية على الحيز الإلكتروني للجريمة، لمعرفة مدى إمكانية استيعاب النصوص التقليدية لهذه الجرائم. وقد توصلنا إلى أنه بالرغم من إمكانية تطبيق النصوص التقليدية على هذه الجرائم الإلكترونية، إلا أننا نفضّل إصدار نصوص خاصة تعنى بهذه الجرائم حتى لا نصطدم في كل مرة إما بمبدأ الشرعية في ظل القواعد العامة، أو الطبيعة اللامادية التي تقوم فيها هذه الجرائم.

إضافة إلى ذلك، يمكن أن تأخذ الجريمة طابعاً نابعاً من طبيعة التعامل الإلكتروني، أين ظهر نوع مستحدث من الجرائم يمس مضمون التعاملات الإلكترونية وبياناتها كالتعدي على نظم المعالجة الآلية للمعطيات وعلى البيانات التي تتضمنها، ما دفع بالمشرع الجزائري إلى إضفاء حماية خاصة على هذه البيانات والمعلومات، أين جرّم جميع الاعتداءات التي تقع على نظم المعالجة الآلية للمعطيات بموجب تعديل قانون العقوبات سنة (2004)، ليقوم بتفعيل حماية جزائية أخرى خص بها التوقيع الإلكتروني من كافة الاعتداءات التي يمكن أن

تمس بحجيته وذلك بتخصيصه فصلا خاصا بالأحكام الجزائية ضمنه في القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين.

وعلى الرغم من أن المشرع الجزائري لم يقرر حماية مباشرة لأدلة الإثبات الإلكتروني في مواجهة جميع الاعتداءات التي قد تطالها وتهز الثقة الواجب توافرها فيها، إلا أنه أضفى حماية غير مباشرة لها عن طريق حماية البيانات والمعلومات المتداولة إلكترونيا سواء بتعديله لقانون العقوبات بإضافة القسم السابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلية لمعطيات، أو بإصداره لقانون التوقيع والتصديق الإلكترونيين.

الخاتمة

الخاتمة

بعد دراستنا لموضوع "**النظام القانوني للإثبات الإلكتروني**"، وهي الدراسة التي كان الهدف الأساسي من ورائها هو بحث وتحليل القواعد القانونية المنظمة لمختلف جوانب الإثبات بالأدلة الإلكترونية المدنية والتجارية، وللحماية المقررة لها من أجل ضمان موثوقيتها في ظل التشريع الجزائري، رغبة منا في محاولة وضع بعض اللبنات التي تساهم في إرساء عناصر نظرية عامة تُعنى بالإثبات الإلكتروني أو على الأقل تبيان ما إذا كانت هناك فعلا نظرية عامة للإثبات الإلكتروني تتسم بالمرونة والقابلية للتعديل، مع تبيان أهم الثغرات القانونية التي وقع فيها المشرع الجزائري وإعطاء مختلف الحلول العملية لمختلف العقبات التي تواجه أدلة الإثبات الإلكتروني مستفيدين في ذلك من تجارب بعض التشريعات المقارنة.

ومن خلال تناول الدراسة لمختلف المسائل القانونية المتعلقة بأدلة الإثبات الإلكتروني، توصلنا لمجموعة من النتائج لعل أهمها ما يلي:

تعتبر المحررات الإلكترونية امتدادا للمحررات التقليدية، وأن اختلاف الدعامة التي تقوم عليها لا تؤدي إلى إنقاص قيمتها في الإثبات إذا ما استوفت الشروط القانونية لقيامها، من تحديد هوية الشخص المنسوب إليه المحرر الإلكتروني، وكذا سلامة هذا الأخير من مخاطر التعديل والتحريف. وهو ما جعل العديد من الدول تصدر قوانين خاصة تُعنى بهذا النوع المستحدث من الأدلة الكتابية، أو القيام بتعديل القواعد القانونية العامة لتشمله وتُقر بحجيته في الإثبات.

أقرت تشريعات الإثبات الإلكترونية عامة، والمشرع الجزائري خاصة، حجية للمحرر الإلكتروني في الإثبات تعادل حجية المحرر التقليدي، وهو ما يطلق عليه بمبدأ التعادل الوظيفي؛ أي أن تكون المساواة كاملة بين المحررات الإلكترونية والمحررات التقليدية، ومتعادلة في المعاملة فيما بينها من حيث الحجية القانونية في مجال الإثبات لدرجة أن يكمل بعضها الآخر، وذلك بغرض إدماج نظام الإثبات الإلكتروني في نظام الإثبات التقليدي واعتبارها نظاما قانونيا واحدا، وكلا لا يتجزأ حتى لا تكون لأحدهما مكانة أقوى أو أضعف بين أدلة الإثبات.

بينا أيضا أن المحررات العرفية الإلكترونية تفتقد للثقة المقررة للمحررات الرسمية الإلكترونية، لذلك أقرت لها تشريعات الإثبات الإلكتروني، وكذا المشرع الجزائري بمرتبة أدنى من المحررات الرسمية؛ سواء من حيث ثبوت حجيتها، أو حتى في طريقة نفيها؛ فالمحررات الرسمية الإلكترونية تعتبر حجة بحد ذاتها ولا يجوز الطعن فيها إلا بالتزوير، في حين أن المحررات العرفية الإلكترونية المعدة للإثبات لا تكون حجة على الغير إلا إذا لم ينكرها صاحبها، أما المحررات العرفية الإلكترونية غير المعدة للإثبات فلا حجية لها إلا إذا أقرها القانون.

توصلنا كذلك إلى أنه على الرغم من إقرار المشرع الجزائري لمبدأ التكافؤ الوظيفي فيما بين المحررات الإلكترونية والمحررات التقليدية، إلا أنه لم ينظم الجانب المتعلق بالمحررات الرسمية الإلكترونية وكيفية إنشائها وحفظها؛ بل على العكس من ذلك؛ فجميع نصوصه التشريعية تؤكد على ضرورة الحضور المادي للموظف العام أثناء إنشاء محرر رسمي، وبذلك فقد أخرج المحررات الرسمية الإلكترونية من دائرة التعامل.

حرصت كل من المؤسسات التشريعية الدولية والإقليمية والوطنية على أهمية الاعتراف بالتوقيع الالكتروني ومنحه نفس الحجية القانونية للتوقيع التقليدي في الإثبات، واعتماد التشريعات السابقة الذكر في تعريفها للتوقيع الالكتروني على المعيار الوظيفي، والالتزام بمبدأ الحياد التقني لتتمكن مستقبلا من استيعاب ما يسفر عنه التقدم العلمي من أنواع وصور جديدة للتوقيع الالكتروني.

كما خلصنا إلى أن التوقيع الإلكتروني بصوره المستحدثة يمكنه أداء نفس الوظائف التي يؤديها التوقيع التقليدي، سواء من حيث تحديد هوية الشخص الموقع أو التعبير عن إرادة صاحب التوقيع، وكذلك ضمان سلامة المحرر. إلا أن هذه الصور المختلفة للتوقيع الإلكتروني تتفاوت فيما بينها على تحقيق هذه الوظائف، وبناء على هذا التفاوت بُنيت مستويات للاعتراف بها من قبل المشرعين، ومنح لكل منها حجية قانونية مناسبة لها في الإثبات.

إن الحجية المقررة لصور التوقيع الإلكتروني غير المستوفية لشروط الموثوقية المحددة قانونا، لا تتساوى مع الاعتراف القانوني المقرر للتوقيع الإلكتروني الموصوف؛ كون هذا

الأخير مُثبت بقوة القانون؛ أي اكتسابه لقرينة قانونية تفيد بصحته؛ على خلاف التوقيع الإلكتروني غير المستوف لشروط الموثوقية؛ أي افتقاده لهذه القرينة القانونية، مما يوجب على من يتمسك به في الإثبات أن يُقدم الدليل على صحته.

لنصل إلى أن حالات التنازع بين الأدلة الكتابية أمر مفروغ منه نتيجة لمبدأ التكافؤ بين الدليلين الكتابيين الورقي والإلكتروني الذي أقرته –أي مبدأ التكافؤ– تشريعات الإثبات الإلكتروني، ومنها المشرع الجزائري، وعلى الرغم من إمكانية حدوث حالات التنازع التي بيّناها سابقا لم تتدخل معظم التشريعات الحديثة لأجل تنظيمها، ما عدا ما نص عليه المشرع الفرنسي والمغربي عند منحهما للقاضي سلطة تقديرية في الترجيح بين الأدلة الكتابية المتعارضة، ليعتمد هذا الأخير في عملية الترجيح على مستوى الثقة والأمان المقرران للتوقيع الإلكتروني الممهور به المحرر الإلكتروني، فكلما كان التوقيع الإلكتروني مستوفيا لجميع الشروط الفنية والتقنية المحددة قانونا كلما تمتع بضمانات موثوقية تفوق أحيانا من حيث الحجية تلك الممنوحة للتوقيع المكتوب، ونتيجة لذلك تغليب كفته عند الترجيح.

أما فيما يخص الشق المتعلق بتأمين أدلة الإثبات الإلكتروني، فقد توصلنا إلى أن المشرع الجزائري قد أقر نوعين من الحماية المقررة لها، حماية تقنية تتمثل أساسا في آليتي التصديق والحفظ الإلكترونيين، وحماية تشريعية جزائية تمثلت في تجريم صور الاعتداء التي يمكن أن تمس بأدلة الإثبات الإلكتروني.

من خلال ما سبق، توصلنا إلى أن آلية التصديق الإلكتروني تعمل على تحقيق مجموعة من الأهداف من بينها، تحديد هوية أطراف المعاملة الإلكترونية، وتحديد أهليتهم للتعامل، وكذا ضمان سلامة وسرية محتوى البيانات المتداولة عبر شبكة الانترنت، مع ضمان عدم إنكار المحررات أو التواقيع الإلكترونية الصادرة من أطراف المعاملة الإلكترونية.

بينما تضمن آلية الحفظ الإلكتروني سلامة المعلومات الواردة في المحرر الإلكتروني من أي تغيير في شكلها الأصلي الذي أنشأت به، أو أرسلت أو استلمت عليه، مع ضمان إمكانية استرجاعه في أي وقت بذات الشكل الذي تم إنشاؤه أو إرساله أو تسلمه عليه، دون أي تحريف أو تبديل أو تغيير.

غير أنه ما يعاب على المشرع الجزائري هو قصوره التشريعي في تنظيم العديد من الجوانب المتعلقة بآلية الحفظ الإلكتروني مقارنة بتنظيمه لآلية التصديق الإلكتروني، حيث أن المرسوم التنفيذي رقم (16-142) المتعلق بحفظ الوثيقة إلكترونيا قد جاء قاصرا على استيعاب جميع المسائل القانونية المتعلقة بالحفظ الإلكتروني، كعدم تحديد الشروط الفنية والقانونية لعملية الحفظ الإلكتروني، وكذا عدم تحديد الجهة المسؤولة عن عملية الحفظ، وكل ما يتعلق بأداء نشاطها، التزاماتها، وكذا تحديد مسؤوليتها.

أما بالنسبة للحماية التشريعية الجنائية المقررة لأدلة الإثبات الإلكتروني، فقد بينا قصور التشريعات المقارنة بصفة عامة، والتشريع الجزائري خاصة عن إيجاد معنى واضح للمال المعلوماتي، بما يساعد على وضع أحكام عامة ضد الجرائم الإلكترونية التي أخذت شكلها من الجرائم التقليدية، وهذا ما جعل القواعد القانونية العامة لمواجهة هذه الجرائم عاجزة عن سد الاعتداءات المختلفة على المعاملات الإلكترونية.

لنصل بعدها إلى أنه على الرغم من أن المشرع الجزائري لم يستحدث نصوصا خاصة لحماية المحررات والتواقيع الإلكترونية من صور الاعتداءات التقليدية – كالتزوير والسرقة مثلا– لم يُقر كذلك بإمكانية تطبيق النصوص العامة المقررة في قانون العقوبات على هذا النوع من الجرائم المستحدثة، وإن كان بالإمكان عمليا تطبيق نصوص التزوير على التزوير الإلكتروني فإن الأمر فيه جدال بالنسبة للسرقة الإلكترونية.

أما بخصوص الحماية الجزائية المقررة بنصوص خاصة، لم نجد المشرع الجزائري قد تطرق إلى حماية المحررات الإلكترونية بشكل مباشر مثلما فعل مع التوقيع الإلكتروني، غير أن حمايته كانت بطريقة غير مباشرة، ذلك من خلال الحماية الجزائية التي أقرها لنظم المعالجة الآلية للمعطيات وكذا للبيانات الإلكترونية، وذلك بتجريمه لمجرد أفعال الدخول والبقاء غير المشروعين للأنظمة المعلوماتية التي تتضمن أدلة الإثبات الإلكتروني، حتى ولو لم يتسبب ذلك في المساس بسلامتهما، كحماية وقائية لهما.

أما بالنسبة للحماية الجنائية المقررة للتوقيع الإلكتروني بموجب القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين، فإنه يؤخذ على المشرع الجزائري إغفاله لتنظيم بعض الجرائم التي تمس بآلية التوقيع الإلكتروني كجريمة التزوير والدخول والبقاء غير المشروع لنظام

التوقيع الإلكتروني، وكذا عدم تجريمه لأفعال الشروع في ارتكاب الجرائم المنصوص عليها والتي تُعد بمثابة حماية وقائية ضد تلك الجرائم.

من خلال ما تطرقنا إليه سابقا في دراستنا هذه؛ خلصنا إلى مجموعة من الاقتراحات نأمل أن تعتمد من طرف المشرع الجزائري نوجزها فيما يلي:

1- تحيين ومراجعة بعض النصوص القانونية ذات الصلة، كقانون مهنة التوثيق والقانون التجاري، بما يتوافق والأحكام التشريعية الجديدة المتعلقة بأدلة الإثبات الإلكتروني.
2- تدارك النقص التشريعي الذي جاء به القانون (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين، حيث كان المفترض أن ينظم المحررات الإلكترونية إلى جانب التوقيع الإلكتروني ويحيط بكافة جوانبها والمسائل المتعلقة بها، وكذا النص على الجرائم الواقعة على التوقيع الإلكتروني والتي تشكل تهديدا مباشرا كجريمة تزوير التوقيع الإلكتروني.
3- تنظيم جميع الجوانب القانونية المتعلقة بالمحررات الرسمية الإلكترونية، والعمل على توفير شبكة تقنية داخلية تربط مكاتب التوثيق والمحضرين القضائيين على مستوى الوطن، لتمكينهم من إنشاء محررات رسمية إلكترونية.
4- إقرار قواعد خاصة لتنظيم حجية المحررات الإلكترونية العرفية تختلف في طبيعتها عن القواعد العامة المطبقة على المحررات العرفية الورقية، بشكل يراعي الضمانات العديدة التي تتوافر فيها، ويمنحها حجية في الإثبات تفوق الحجية المقررة للمحررات الورقية.
5- وضع الضوابط اللازمة للتمييز بين أصل المحررات الإلكترونية وصورتها.
6- التنظيم الدقيق لجوانب الحفظ الإلكتروني للمحرر والتوقيع في الشكل الإلكتروني، على غرار نشاط التصديق الإلكتروني، مع تحديد الجهات المكلفة به.
7- إدخال تعديلات على قانون العقوبات الجزائري بما يسمح باستيعاب الجرائم المستحدثة كالتزوير والسرقة والنصب والاحتيال وخيانة الأمانة في مجال المعاملات الإلكترونية.
8- إصدار ما تبقى من المراسيم التنظيمية للقانون (15-04) والتي لم تصدر لحد الساعة.

الفهرس

العنوان.....الصفحة
مقدمة.....09
الباب الأول: القيمة القانونية لأدلة الإثبات الإلكتروني.....17
الفصل الأول: المحررات الإلكترونية 19
المبحث الأول: ماهية المحررات الالكترونية.....**21**
المطلب الأول: مفهوم المحررات الالكترونية.....**22**
الفرع الأول: التعريف بالمحررات الالكترونية في الفقه والتشريع. **22**
أولا: التعريف الفقهي للمحررات الإلكترونية.....**23**
ثانيا: تعريف المحررات الالكترونية في التشريع الدولي.....**24**
ثالثا: تعريف المحررات الإلكترونية في بعض التشريعات الوطنية المقارنة.....**25**
الفرع الثاني: محددات المحرر الإلكتروني **32**
أولا: عناصر المحرر الإلكتروني.....**32**
1- الكتابة الإلكترونية.....**32**
2- التوقيع الإلكتروني.....**36**
ثانيا: شروط صحة المحرر الإلكتروني..... **36**
1- قابلية المحرر الإلكتروني للقراءة.....**37**
2- شرط سلامة المحرر الإلكتروني.....**38**
3- كشف هوية مُصدر المحرر.....**41**

المطلب الثاني: صور المحررات الإلكترونية.....**43**
الفرع الأول: صور المحررات الإلكترونية غير المرتبطة بشبكة الإنترنت.....**43**
أولا: مُخرجات الهاتف (التسجيل الصوتي).....**44**
ثانيا: مُخرجات التلكس والفاكس.....**45**
1 – مُخرجات التلكس.....**45**
2 – مُخرجات الفاكس.....**47**
ثالثا: مُخرجات الحاسوب.....**47**
1- المخرجات الورقية.....**48**
2- المُخرجات الإلكترونية.....**48**
رابعا: الدفاتر التجارية الإلكترونية.....**50**
الفرع الثاني: صور المحررات الإلكترونية المرتبطة بشبكة الانترنت..... **52**
أولا: البريد الإلكتروني.....**52**
1 - رسائل البريد الإلكتروني غير الموقعة.....**54**
2-رسائل البريد الإلكتروني الموقعة إلكترونيا.....**55**
3- رسائل البريد الإلكتروني الموصى عليها.....**55**
ثانيا: رسائل الانترنت.....**56**

المبحث الثاني: حجية المحررات الإلكترونية في الإثبات..... 59
المطلب الأول: القيمة الثبوتية للمحررات الرسمية الإلكترونية..... **60**
الفرع الأول: شروط صحة المحرر الرسمي الإلكتروني..... **61**
الفرع الثاني: عناصر حجية المحرر الرسمي الإلكتروني..... **.64**
أولا: حجية المحررات الرسمية الإلكترونية بالنسبة للأشخاص.....**64**
ثانيا: حجية المحررات الرسمية الإلكترونية بالنسبة للبيانات الواردة فيها.....**66**
1- البيانات التي لا يجوز الطعن في حجيتها إلا بالتزوير.....**66**
2- البيانات التي يجوز إثبات عكسها وفقا للقواعد العامة في الإثبات.....**67**
ثالثا: حجية المحررات الرسمية الإلكترونية من حيث صدورها ممن وقعها وسلامتها المادي68
الفرع الثالث: حجية صور المحررات الرسمية الإلكترونية..... **69**
أولا: الشروط الواجب توافرها لإصدار صورة ورقية من محرر إلكتروني.....**71**
ثانيا: الشروط الواجب توافرها لإصدار صورة إلكترونية من محرر إلكتروني.....**72**
ثالثا: إصدار نسخة إلكترونية من محرر ورقي.....**72**

المطلب الثاني: القيمة الثبوتية للمحررات العرفية الإلكترونية.....**75**
الفرع الأول: حجية المحررات العرفية الإلكترونية المُعدّة للإثبات **76**
أولا: المساواة المطلقة بين المحرر العرفي الإلكتروني والمحرر العرفي الورقي..... **76**
1- حجية المحرر العرفي الإلكتروني من حيث صدوره ممن وقع عليه..... **77**
2- حجية المحرر العرفي الإلكتروني من حيث قوة البيانات المدونة فيه.....**79**
3- حجية تاريخ المحرر العرفي الإلكتروني..... **80**
ثانيا: عدم المساواة بين المحرر العرفي الإلكتروني والمحرر العرفي الورقي **82**
الفرع الثاني: حجية المحررات العرفية الإلكترونية غير المُعدّة الإثبات.....**84**
أولا: حجية رسائل الفاكس والتلكس.....**85**
ثانيا: حجية رسائل البريد الإلكتروني.....**88**
1- حجية رسائل البريد الإلكتروني غير الموقعة.....**88**
2- حجية رسائل البريد الإلكتروني الممهورة بتوقيع.....**89**
3- حجية رسائل البريد الإلكتروني الموصى عليها.....**89**
ثالثا: حجية الدفاتر التجارية الإلكترونية.....**90**

الفصل الثاني: الاعتراف التشريعي بالتوقيع الإلكتروني في الإثبات.....93
المبحث الأول: ماهية التوقيع الإلكتروني.....95
المطلب الأول: مفهوم التوقيع الإلكتروني..... **96**
الفرع الأول: التعريف الفقهي والقضائي للتوقيع الإلكتروني.....**96**
أولا: التعريف الفقهي للتوقيع الإلكتروني.....**97**
ثانيا: التعريف القضائي للتوقيع الإلكتروني.....**100**
الفرع الثاني: التعريف القانوني للتوقيع الإلكتروني.....**102**
أولا: تعريف التوقيع الإلكتروني في التشريعات الدولية.....**102**
1 – لجنة الأمم المتحدة للقانون التجاري الدولي (اليونسترال).....**102**

2 – التوقيع الإلكتروني في التوجيهات الأوروبية.....**103**
ثانيا: تعريف التوقيع الإلكتروني في التشريعات الوطنية.....**106**

المطلب الثاني: صور ووظائف التوقيع الإلكتروني.....**114**
الفرع الأول: صور التوقيع الالكتروني.....**115**
أولا: التوقيع الرقمي.....**115**
1- التشفير التماثلي..... 117
2- التشفير اللاتماثلي.....117
ثانيا: التوقيع البيومتري.....**119**
ثالثا: التوقيع الكودي.....**120**
رابعا: التوقيع بالقلم الالكتروني..... **123**
1 - الوظيفة الأولى: وظيفة التقاط التوقيع.....**124**
2- الوظيفة الثانية: التحقّق من صحة التوقيع **125**
الفرع الثاني: مدى تحقق وظائف التوقيع في صور التوقيع الإلكتروني.....**126**
أولا: تحديد هوية الموقع **127**
ثانيا: قدرة التوقيع الإلكتروني على إثبات قبول الموقع على مضمون المحرر الإلكتروني **131**
ثالثا: قدرة التوقيع الإلكتروني على التحقّق من سلامة محتوى ما تم التوقيع عليه **132**

المبحث الثاني: حجية التوقيع الإلكتروني في الإثبات.....**135**
المطلب الأول: شروط حجية التوقيع الإلكتروني في الإثبات.....**136**
الفرع الأول: الشروط الشخصية لصحة التوقيع الإلكتروني.....**136**
الفرع الثاني: الشروط الموضوعية لصحة التوقيع الإلكتروني.....**140**
أولا: شرط سيطرة الموقع الحصرية على وسائل إنشاء التوقيع الإلكتروني.....**140**
ثانيا: شرط كشف التوقيع الإلكتروني لأي تعديل أو تغيير لاحق للبيانات المدرج عليها.....**144**
ثالثا: شرط إنشاء الوقيع الإلكتروني بواسطة آلية إنشاء توقيع إلكتروني مؤمنة.....**146**
رابعا: شرط اعتماد التوقيع الإلكتروني على شهادة تصديق إلكتروني موصوفة.....**151**

المطلب الثاني: أثر تفاوت صور التوقيع الإلكتروني على حجية المحررات الإلكترونية... **155**
الفرع الأول: دور القاضي في الترجيح بين الأدلة الكتابية المتعارضة.....**155**
الفرع الثاني: دور التوقيع الإلكتروني في الترجيح بين الأدلة الكتابية.....**158**
أولا: التعارض بين محرر عرفي إلكتروني موصوف ومحرر عرفي ورقي.....**159**
ثانيا: التعارض بين محرر عرفي إلكتروني بسيط ومحرر عرفي ورقي.....**160**
ثالثا: التعارض بين محرر عرفي إلكتروني موصوف ومحرر رسمي ورقي.....**162**
رابعا: التعارض بين محرر رسمي إلكتروني ومحرر رسمي ورقي.....**163**
خلاصة الباب الأول.....**166**

الباب الثاني: الحماية المقررة لأدلة الإثبات الإلكتروني..... .....**170**
الفصل الأول: الآليات التقنية لحماية أدلة الإثبات الإلكتروني..... .....**172**

المبحث الأول: دور الحفظ والتصديق الإلكترونيين في تأمين أدلة الإثبات لإلكتروني.... 174.
المطلب الأول: الحفظ الإلكتروني.....**176**
الفرع الأول: تعريف الحفظ الإلكتروني.....**176**
الفرع الثاني: شروط الحفظ الإلكتروني.....**183**
أولا: شروط تتعلق ببيانات الوثيقة الإلكترونية.....**183**
ثانيا: الشروط المتعلقة بدعامة الحفظ.....**185**
ثالثا: مدة الحفظ الإلكتروني.....**187**
الفرع الثالث: المسؤول عن عملية الحفظ الإلكتروني..... .....**188**

المطلب الثاني: التصديق الإلكتروني.....**190**
الفرع الأول: الجهات المكلفة بتقديم خدمة التصديق الإلكتروني..... ..... **191**
الفرع الثاني: نظام ترخيص وتفويض جهات التصديق الإلكتروني..... .....**197**
أولا: الترخيص للممارسة مهنة التصديق الإلكتروني.....**197**
ثانيا: التفويض للممارسة مهنة التصديق الإلكتروني.....**205**
الفرع الثالث: شروط ممارسة نشاط مؤدي خدمات التصديق الإلكتروني **207**

المبحث الثاني: الآثار القانونية المترتبة عن عملية التصديق الإلكتروني.....213
المطلب الأول: التزامات مؤدي خدمات التصديق الإلكتروني..... **214**
الفرع الأول: الالتزامات المتعلقة بصحة وسرية البيانات الشخصية للموقع.....**214**
أولا: الالتزام بالتحقق من صحة البيانات **215**
ثانيا: الالتزام بالحفاظ على سرية البيانات..... **218**
الفرع الثاني: الالتزامات المتعلقة بشهادة التصديق الإلكترونية.....**221**
أولا: الالتزام بإصدار شهادة التصديق الإلكتروني.....**221**
1-تعريف شهادة التصديق الإلكتروني.....**221**
2-البيانات الواجب توفرها في شهادة التصديق الإلكتروني.....**225**
ثانيا: الالتزام بتعليق أو إلغاء شهادة التصديق الإلكتروني.....**228**
1- حالات تعليق العمل بشهادة التصديق الإلكتروني.....**229**
2- حالات إلغاء العمل بشهادة التصديق الإلكتروني.....**230**

المطلب الثاني: المسؤولية المدنية لمؤدي خدمات التصديق الإلكتروني..... **234**
الفرع الأول: مسؤولية مؤدي خدمات التصديق الإلكتروني وفقا للقواعد العامة.....**235**
أولا: المسؤولية العقدية لمؤدي خدمات التصديق الإلكتروني.....**235**
1- الخطأ العقدي.....**236**
2- الضرر..**237**
3- العلاقة السببية.....**238**
ثانيا: المسؤولية التقصيرية لمؤدي خدمات التصديق الإلكتروني.....**239**
1- مسؤولية مؤدي الخدمات عن فعله الشخصي.....**240**
2- مسؤولية مؤدي الخدمات عن أخطاء تابعيه.....**241**

3- مسؤولية مؤدي الخدمات عن الأشياء غير الحية.....**242**
الفرع الثاني: مسؤولية مؤدي خدمات التصديق الإلكتروني وفقا للقواعد الخاصة..... **243**

الفصل الثاني: الحماية الجزائية لأدلة الإثبات الإلكتروني.....252
المبحث الأول: الحماية الجزائية لأدلة الإثبات الإلكتروني في إطار الجرائم التقليدية.....254
المطلب الأول: جريمة التزوير الإلكتروني.....255
الفرع الأول: مفهوم جريمة التزوير الإلكتروني **255**
أولا: تعريف التزوير الإلكتروني.....**256**
ثانيا: خصائص التزوير الإلكتروني.....**259**
1- صعوبة الكشف عن جريمة التزوير الإلكتروني.....260
2- جريمة عابرة للحدود.....260
3- تفرّد صفة الجاني.....**261**
الفرع الثاني: البناء القانوني لجريمة التزوير الإلكتروني **261**
أولا: الركن المادي.....**262**
1- السلوك المادي لجريمة التزوير الإلكتروني.....**262**
2- الضرر المترتب عن تغيير الحقيقة.....**266**
ثانيا: الركن المعنوي.....**267**
1- القصد الجنائي العام.....**267**
2- القصد الجنائي الخاص.....**268**

المطلب الثاني: جريمة السرقة المعلوماتية.....**270**
الفرع الأول: محل جريمة السرقة المعلوماتية.....**272**
أولا: مدى اعتبار المعلومات محلا لجريمة السرقة قضائيا.....**272**
1- الاتجاه الرافض لفكرة الاعتراف بقابلية المعلومات كمحل لجريمة السرقة.....272
2- الاتجاه المؤيد لفكرة الاعتراف بقابلية المعلومات كمحل لجريمة السرقة.....273
ثانيا: مدى اعتبار المعلومات محلا لجريمة السرقة فقهيا.....**275**
1- شروط حماية المعلومات جنائيا.....**276**
2- الاتجاه الفقهي الرافض لاعتبار المعلومات محلا لجريمة السرقة.....278
3- الاتجاه الفقهي المؤيد لاعتبار المعلومات محلا لجريمة السرقة.....**280**
الفرع الثاني: أركان جريمة السرقة المعلوماتية.....**282**
أولا: الركن المادي لجريمة السرقة المعلوماتية.....**282**
ثانيا: الركن المعنوي لجريمة السرقة المعلوماتية.....**286**

المبحث الثاني: الحماية الجزائية لأدلة الإثبات الإلكتروني في إطار الجرائم المستحدثة....289
المطلب الأول: الحماية الجزائية في ظل جرائم المساس بأنظمة المعالجة الآلية للمعطيات...290
الفرع الأول: جريمة الدخول أو البقاء غير المشروع في النظام.....**290**
أولا: الركن المادي للجريمة **291**
1- مفهوم الدخول إلى النظام والبقاء غير المشروع فيه.....**292**

2- صورتا الركن المادي.....**295**
ثانيا: الركن المعنوي للجريمة.....**296**
ثالثا: عقوبة الجريمة.....**298**
الفرع الثاني: جريمة التلاعب غير المصرح به بالمعلومات.....**299**
أولا: الركن المادي لجريمة التلاعب غير المصرح به بالمعلومات.....**299**
1- السلوك الإجرامي.....**300**
2- محل النشاط الجرمي.....**303**
3- النتيجة الإجرامية.....**304**
ثانيا: الركن المعنوي لجريمة التلاعب غير المصرح به بالمعلومات.....**304**
الفرع الثالث: جريمة التعامل في معلومات غير مشروعة.....**305**
أولا: الركن المادي لجريمة التعامل غير المشروع في المعلومات.....**306**
1- التعامل في معلومات صالحة لارتكاب جريمة.....**306**
2- جريمة التعامل في معلومات متحصلة من جريمة.....**309**
ثانيا: الركن المعنوي لجريمة التعامل غير المشروع في المعلومات.....**311**

المطلب الثاني: الحماية الجزائية في ظل قانون التوقيع والتصديق الإلكترونيين.....**312**
الفرع الأول: الجرائم الماسة بتداول البيانات.....**313**
أولا: جرائم انتهاك سرية وخصوصية البيانات **313**
1- جريمة التعامل غير المشروع ببيانات توقيع إلكتروني موصوف.....**313**
2- جريمة إفشاء بيانات شهادة التصديق الإلكتروني.....**316**
3- جريمة جمع البيانات الشخصية للموقع واستخدامها في غير غرضها.....**318**
4- جريمة كشف معلومات سرية أثناء التدقيق.....**321**
ثانيا: جرائم إساءة استخدام شهادة التصديق الإلكتروني.....**325**
1- جريمة الإدلاء بإقرارات كاذبة.....**325**
2- جريمة الاستخدام غير المشروع لشهادة التصديق الإلكتروني.....**328**
الفرع الثاني: الجرائم الماسة بنشاط التصديق الإلكتروني.....**330**
أولا: جريمة عدم تحديد هوية طالب شهادة التصديق.....**330**
ثانيا: جريمة عدم إبلاغ السلطة الاقتصادية بالتوقف عن النشاط.....**333**
ثالثا: جريمة ممارسة نشاط التصديق الإلكتروني بدون ترخيص.....**336**
خلاصة الباب الثاني 341

خاتمة 345
قائمة المراجع.....351
الفهرس.....376

الملخص:

أدى التطور التكنولوجي الحاصل في مجال تكنولوجيا المعلومات وقطاع الاتصالات إلى ظهور معاملات لم تكن معروفة سابقا، إذ أصبح بإمكان الأشخاص إبرام العقود بجميع أنواعها وإنشاء التصرفات القانونية عن بعد، وهو ما يطلق عليها بالمعاملات الإلكترونية والتي تعتمد أساسا في قيامها على المحررات والتواقيع في الشكل الإلكتروني.

إن حداثة المعاملات الإلكترونية أدت إلى تخوف الأفراد من الدخول فيها، إما بسبب التخوف من عدم موثوقيتها أو بسبب عدم قدرتهم على إثباتها، مما زاد من أهمية الحديث عن دور أدلة الإثبات الإلكتروني ومدى حجيتها في الإثبات خصوصا المحررات والتواقيع في الشكل الإلكتروني، حيث صارت محط اهتمام بالغ من الفقه والقضاء والتشريع دوليا وإقليميا ووطنيا.

الكلمات المفتاحية: الإثبات التقليدي، الإثبات الإلكتروني، المحررات الإلكترونية، التوقيع الإلكتروني.

Résumé

L'évolution numérique dans les domaines de technologies de l'information et de la communication (TIC) à entrainer l'émergence de transactions jusqu'alors inconnues. Désormais, les personnes peuvent conclurent de différents contrats à distance; il s'agit alors de transactions électroniques établies sous forme de documents et signature électronique.

La croissance fulgurante des transactions électroniques aujourd'hui laisse les individus méfiants à cette nouvelle forme de contractualisation à distance. En effet, cette méfiance est liée sans aucun doute aux questions relatives à la fiabilité de la signature et à la certification électroniques. C'est la raison pour laquelle, les transactions électroniques demeurent le centre d'intérêt de la loi, la doctrine et de la jurisprudence tant au niveau national qu'international.

Mots clé : preuve traditionnelle, preuve électronique, actes électroniques, signature électronique.

Abstract:

The technological development in the field of Information Technology and the Telecommunications sphere has brought forth the emersion of transactions that were not formerly known, as people can conclude contracts of all kinds and establish legal actions remotely, hence they are called electronic transactions, which rely fundamentally in its establishment on the electronic-based documents and Signatures.

The novelty of electronic transactions induced a trepidation among individuals that held them back from entering into it, either because of its lack of reliability or because of their inadequacy to prove it, which increased the importance of discussing the role of the evidences of the electronic substantiation and the extent of its argument in proof, especially the documents and signatures in the electronic form, that it grabbed the attention of the Jurisprudence, Judiciary and Legislation internationally, regionally and nationally.

Key words: traditional proof, electronic proof, electronic documents, electronic signature.